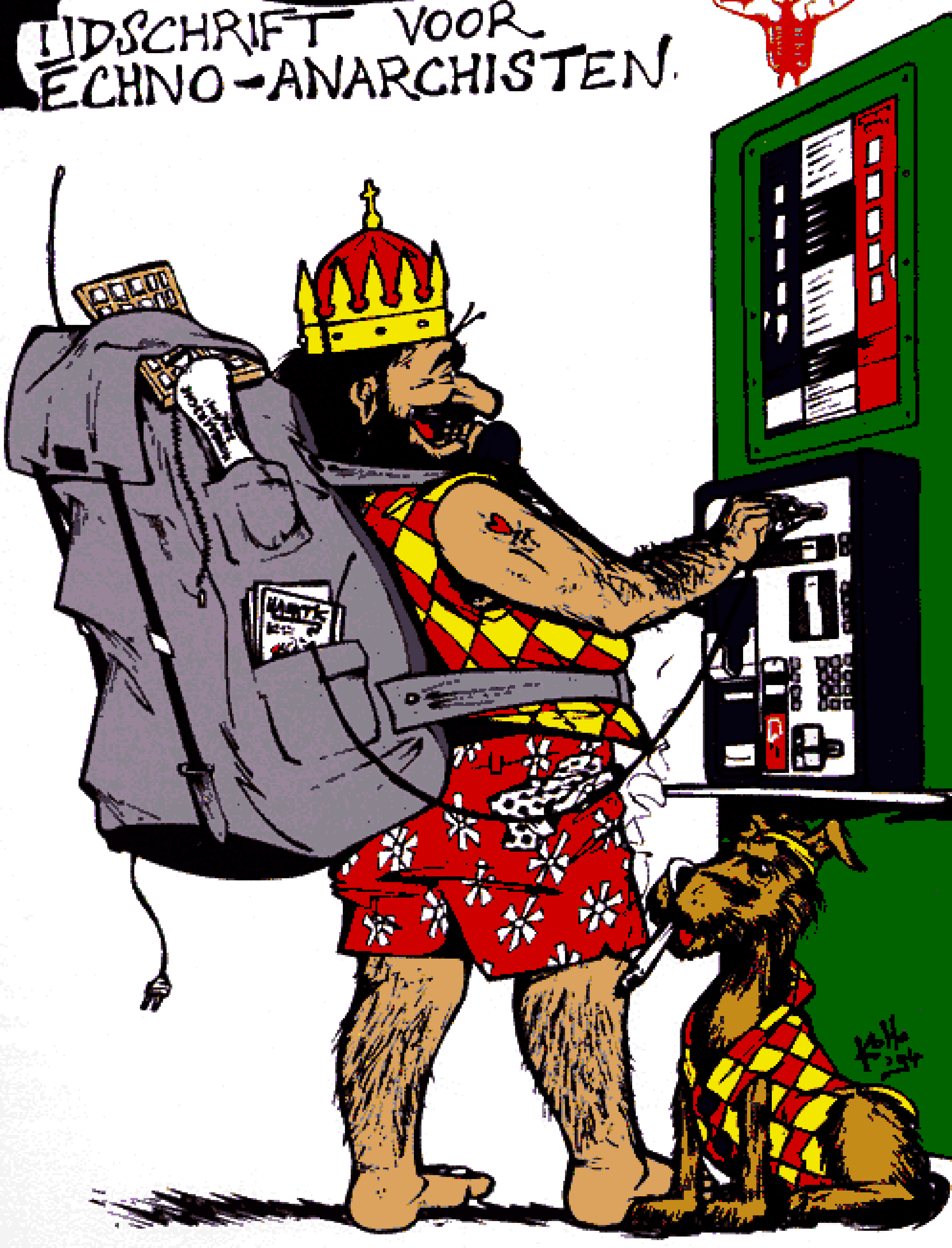
WE ARE EVERYWHERE

f 8,-

HACK-TIC

24-25

TIJDSCHRIFT VOOR TECHNO-ANARCHISTEN.



Het blad voor de vrije techneut

COLOFON

Hack-Tic is Nederlands eerste hackerblad. Het verschijnt zonder enige regelmaat. Het eerste nummer verscheen 13 januari 1989. Tics 5/6, 9/10, 11/12, 14/15, 16/17, 18/19, 20/21, 22/23 en 24/25 zijn dubbeldik.

UITGAVE: Dit keer met extreem veel moeite door de stichting Hack-Tic. Een onderdeel van Hack-Tic Holding Bonaire Inc.
ISSN: 0926-0269
MET DANK AAN: Cor (BOFH), The Key, Benten, Billsf, Carla, Alex, The Dude, Herman Acker, Peter Poelman, B. King, Xokum 3, Ing. (Cum Laude), Karin, Hanneke, Erik, Paul, Dial-Tone, RGB, Joost, PTT, de 'Stamp-On Stuff-In Mail-Out'-crowd, de mensen van XS4ALL, en iedereen die we vergeten zijn. Het lek binnen uw eigen organisatie zit trouwens hoger dan u denkt.
ONDANKS: Jos, Ko, Bierman, Wilmans, Valente
ZWEEP: Carla
ILLUSTRATIES: Koen Hottentot.
HOOFDVERDACHTE: Rop Gonggrijp
C. V.: Archibald Tuttle

KONTAKT: De redaktie is waarschijnlijk nauwelijks te bereiken via:
Postbus 22953
1100 DL Amsterdam.
Internet e-mail werkt beter: **redaktie@hacktic.nl**
Telefoon: **020-6222699**, Fax: **020-6222753**

PRIJS: Losse nummers kosten 4 gulden en 50 cent, een abonnement voor 10 nummers (of 5 dubbelnummers, net waar we zin in hebben) kost 40 piek. Dit is een dubbelnummer en kost *f*8,-. Abonnementsgelden kun je overmaken op gironummer 6065765 t.n.v. de Stichting Hack-Tic. Abonnementen beginnen met het volgende nummer.

ZAKELIJK TARIEF: Bedrijven en instellingen betalen 100 piek voor 10 nummers. Kassa!

INTERNATIONAL RATES: Outside Holland or Belgium, 10 issues cost US$ 35, DM 60. Payment in cash ONLY to Hack-Tic, P.O. Box 22953, 1100 DL Amsterdam, The Netherlands.
Cheques of ANY kind are used as toilet paper!

ABONNEMENT VOOR HET LEVEN: Voor *f* 375,- heb je een levenslang abonnement op Hack-Tic dat zelfs na de dood testamentair op een ander kan overgaan. Het abonnement duurt zolang Hack-Tic duurt. Nooit meer gezeur met het verlengen van je abonnement! Buitenlandse levens-abos krijgen een gratis woordenboek van Nederlands naar de taal van hun keuze. Als je abonnee voor het leven wordt krijg je alle oude nummers (voor zover voorradig) thuis gestuurd.

PRIVACY: Het is natuurlijk via onze bankafschriften makkelijk na te gaan wie er abonnee zijn. Heb je een maatschappelijke positie die je niet wilt verliezen, of ben je gewoon paranoide, dan kun je ook geld en adres in een envelop stoppen en die aan onze postbus (zie 'kontakt') sturen, wij weten dan genoeg. De Hack-Tic wordt altijd verstuurd in een neutrale envelop, en het abonneebestand is op onze disks versleuteld. Hack-Tic is ook verkrijgbaar bij de goede boekhandel.

DISCLAIMER: De informatie in Hack-Tic dient slechts een educatief doel. Gebruik van deze informatie zou strafbaar/staatsgevaarlijk/stout kunnen zijn. De redaktie wijst iedere verantwoordelijkheid voor gebruik door lezers van de in Hack-Tic opgenomen informatie af. De mening van een auteur weerspiegelt niet noodzakelijkerwijs de mening van de redaktie of uitgever.

NADRUK: toegestaan! Kranten, tijdschriften, omroeporganisaties, politieke partijen, wasmachinereparateurs etc. mogen zonder voorafgaande toestemming van de redaktie (maar natuurlijk wel met bronvermelding) stukken overnemen uit Hack-Tic. De bovenstaande disclaimer blijft echter van kracht. Nadruk van de gehele Hack-Tic is natuurlijk verboden.

NABESTELLEN: Hack-Tic's 1 t/m 20-21 zijn alleen nog te krijgen door alle oude nummers te bestellen. Dit pakket kost fl. 100,- en wordt onder rembours verstuurd. Voor latere nummers 8 piek overmaken o.v.v. het gewenste nummer.

HOE: Deze Hack-Tic werd met Framemaker 3.0 (onder Windows) gemaakt op een 386 met 16 MB geheugen. De plaatjes werden met een geleende HP ScanJet opgezogen en print-outs van elke pagina werden met een OKI OL-400 gezoelt en daarna ambachtelijk gedrukt. De voorplaat komt uit Coreldraw 4.0 en ging op floppy naar de drukker. Toen hebben we het nog even ergens laten vouwen, nieten en snijden en klaar was Kees.

Gefopt!

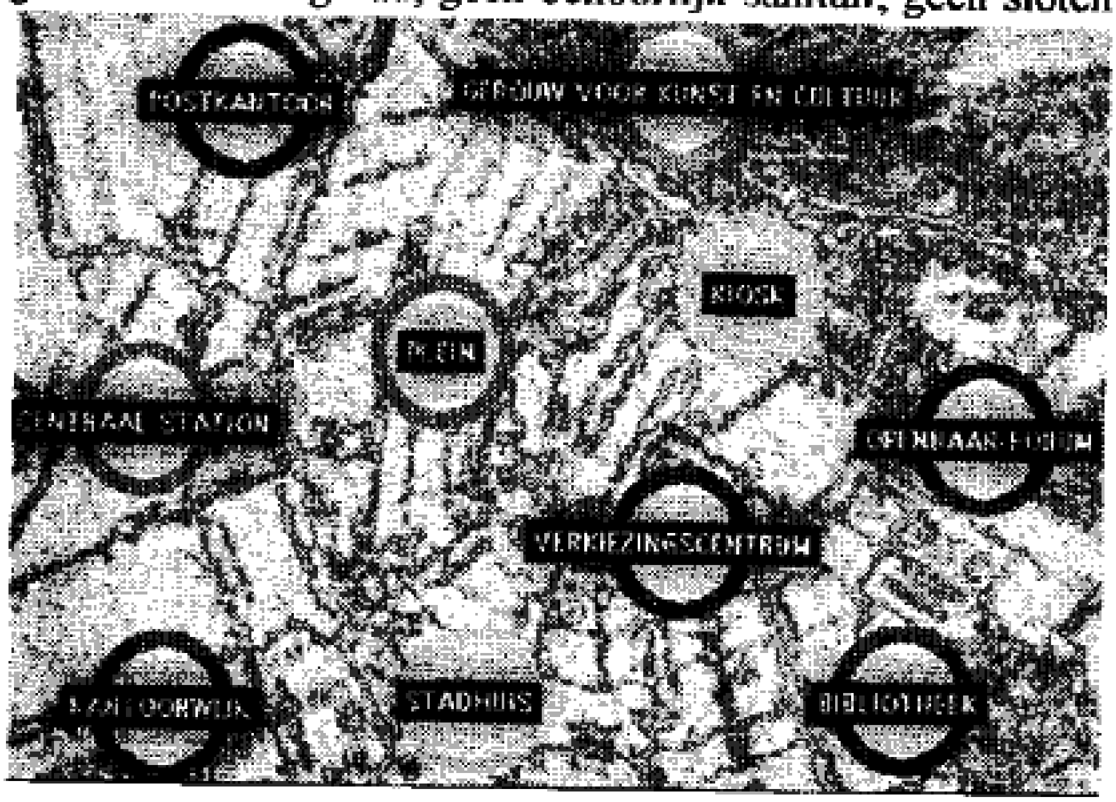
We zijn weer eens zo laat dat precies de helft van onze abonnees denkt dat we niet meer bestaan.

We dachten dat de meeste abonnees de truuk ondertussen wel door zouden hebben en dus hebben we deze keer iets meer moeite gedaan om de indruk te wekken dat we niet meer bestaan. We zijn namelijk verhuisd, en zowel het telefoonnummer als het faxnummer zijn veranderd. We zitten nu in een statig pand aan de Prins Hendrikkade in Amsterdam, maar daarover straks meer. Ons nieuwe telefoonnummer is 020-6222699, ons faxnummer is 020-6222753. Meer creatieve manieren om ons te bereiken vind je in het colofon op de pagina hiernaast. Welkom in Hack-Tic 24-25 overigens..... Wat is er allemaal gebeurd de laatste tijd?

De Digitale Stad (020-6225222)

Het project 'De Digitale Stad' dat afgelopen januari van start ging is een klein beetje uit de hand gelopen (in positieve zin). Marleen Stikker van cultureel centrum De Balie en Felipe Rodriquez van Hack-Tic Netwerk hebben met 'hun' project het een en ander bereikt. Om maar wat te noemen: een 'openbare ruimte' op het Internet waar naar hartelust geëxperimenteerd wordt met nieuwe vormen van communicatie, een platform voor kunst en cultuur op het net, het openbreken van de databases met openbare bestuurlijke informatie, maatschappelijke erkenning voor hackers (die het project mede mogelijk hebben gemaakt), en subsidie om door te gaan en verder te bouwen. Inmiddels is De Digitale Stad een vertrouwde omgeving voor duizenden mensen en werken honderden mensen op de een of andere manier mee om de stad nog mooier te maken.

Terug naar de dag voordat De Digitale Stad van start ging. De PTT moest lijnen aanleggen in een pand dat geen verwarming had, geen behoorlijk sanitair, geen sloten op de deuren (een gammel hangslotje daargelaten) en nog maar net plafonds in (sommige) ruimtes. Hoe dat allemaal kwam is een lang verhaal, maar laten we het er op houden dat er in Amsterdam een aannemer, een architekt en een huiseigenaar wonen die wat ons betreft met z'n drietjes



onder een bus mogen lopen.
In dit fijne pand stonden in een oud 19-inch rek, tussen het bouwstof (geen grapje), twee Solair (SUN-kloon) machines en een kudde modems. We hadden voor XS4ALL 20 modemlijnen besteld, en voor DDS 8. Door een foutje van de PTT kreeg het (inmiddels gepubliceerde) nummer van DDS de 20 en XS4ALL 8.
Gevolg was dat XS4ALL enige weken nog onbereikbaarder was dan anders, en De Digitale Stad ook. DDS werd namelijk nogal vaak gebeld. Als de machine door koukleumende systeembeheerders na onderhoud weer werd aangezet dan waren alle modems in luttele seconden bezet. De maximale tijd dat mensen binnen mochten zijn werd van van een uur naar een half uur teruggebracht, maar ook dat hielp nauwelijks: de machine zat gewoon vol.

XS4ALL (020-6222175 of 020-6265060)

Inmiddels heeft DDS 25 telefoonlijnen, en ook de capaciteit van de Internet host XS4ALL is flink toegenomen: daar hangen nu 22 lijnen aan. En ook die zijn vaak nog bezet, dus er komen binnenkort nog meer lijnen bij. De groei van onze netwerkactiviteiten is op meer vlakken nauwelijks bij te benen: we hebben een 144 kbit verbinding naar het Internet, en er gaat nu elke maand meer dan 9 GigaByte aan Internet-verkeer door onze gateway. Inmiddels werken er in het beheer van XS4ALL en DDS vijf mensen op loonbasis, is er een stagiaire aangenomen en werkt er een aantal dappere vrijwilligers om het allemaal nog mooier te maken.
Met andere woorden: de Mega-Internetprovider Hack-Tic Netwerk is veel groter gegroeid dan het kleine tijdschriftje dat ooit aan de wieg heeft gestaan. Hoewel er altijd sterke banden tussen het tijdschrift Hack-Tic, De Digitale Stad en Hack-Tic Netwerk zullen zijn, zijn het nu allemaal zelfstandige organisaties die hun eigen weg volgen. Het is volgens alle betrokken partijen beter om meerdere (waar mogelijk samenwerkende) clubjes te zijn. De Stichting Hack-Tic Netwerk heet dan ook sinds kort Stichting XS4ALL, een naam die de lading veel beter dekt.

Vernieuwd Voicemail Systeem (020-6222699)

Ook modemlozen kunnen nog bij ons terecht: iedere abonnee krijgt gratis een postbus op ons vernieuwde Voicemail systeem. Er draait nu al een beperkt informatiesysteem op het bovenstaande nummer, maar eind september wordt het allemaal nog veel leuker. Je kunt dan, als je Hack-Tic abonnee bent, je eigen postbus krijgen. Op het Hack-Tic Voicemail systeem kun je direct in kontakt komen met andere Hack-Tic lezers, en het kost niet eens 1 gulden per minuut. Bewaar het label op de envelop waarin je deze Hack-Tic kreeg of word snel abonnee.
Er zijn zelfs al plannen om het Voicemail Systeem van een e-mail koppeling te voorzien, zodat je korte e-mail berichten gesproken in je mailbox ontvangt. Verder zijn we de mogelijkheden van 'fax-on-demand' aan het onderzoeken, zodat lezers met een fax allerlei informatie op kunnen vragen.

WWW-server (http://www.hacktic.nl/magazine)

Wie nog geen modem heeft moet er toch ernstig over denken om er eentje aan te schaffen: vanaf medio september '94 draaien we een World-Wide-Web server op het Internet adres http://www.hacktic.nl/magazine. De webserver komt net als het papieren tijdschrift vol te staan met leuke tips en truuks, tekeningen van KoHo en nog veel meer. Meer informatie over World-Wide-Web en over hoe je op je eigen PC mee kunt doen vind je op pagina 43.

Het tijdschrift

HackTic

onregelmatig
ondeugend
nu ook on-line

Oude Hack-Tics

nu in luxe verzameldoos!

Je kunt nu ALLE oude nummers van Hack-Tic bestellen. Denk je eens in: meer dan 600 pagina's Hack-Tic. En dat voor maar f100,- incl. verzendkosten. Je krijgt er dan ook nog een luxe verzameldoos van grijs recyclingkarton bij. Je bestelt door 100 piek over te maken op giro 6065765 t.n.v. Hack-Tic onder vermelding van je naam, adres en 'pakket'

CD-ROMs gekraakt

De laatste uitgave van het blad 'Die Datenschleuder' van de Chaos Computer Club in Duitsland heeft een artikel over het kraken van software CD-ROMs.
Een aantal producenten verkoopt voor weinig of geen geld CD-ROMs met daarop tientallen software-pakketten die je pas kunt gebruiken als je betaalt. Yellow-point maakt zo'n Pay-CD-ROM, maar ook IBM doet mee met haar 'Showcase' CD-ROM. De software op zo'n CD-ROM is versleuteld, alleen de demo versie is toegankelijk. Wie betaalt krijgt de sleutel om de echte versie van de software te decoderen.

Altijd dezelfde sleutel

De Duitse hackers mogen geen software disassembleren, daar hebben ze in Duitsland wetten tegen. Gelukkig heeft de Chaos Computer Club ook leden in Bulgarije, en die hebben het hele zaakje eens even onderzocht. Het werkt als volgt:
Software is op schijf met behulp van het algoritme DES versleuteld met sleutel A.
Klant runt 'ik-wil-een-stuk-software-kopen-programma'. Dit programma geeft op het scherm het telefoonnummer dat gebeld moet worden, en een willekeurig getal X. De klant belt op en geeft zijn credit-card nummer. Als het nummer klopt (credit-card betrouwbaarheid is een heel ander verhaal) dan berekent de software bij de leverancier het getal Y, en dat wordt de klant medegedeeld.
Het getal Y is zo berekend dat X en Y samen te herleiden zijn tot de sleutel A waarmee het programma is gecodeerd. De klant tikt Y in en het gekochte programma wordt vervolgens door de software bij de klant gedecodeerd en op de harddisk geschreven. Iedere klant heeft dus een andere X en Y, maar ze leiden elke keer weer tot dezelfde A. Dit is gedaan omdat het maken van enkele CD-ROMs veel te duur is, er moet dus wel elke keer dezelfde sleutel gebruikt worden.
De Chaos-lieden hebben een programma gemaakt dat de werkelijke code A van een aantal bekende merken CD-ROMs afvangt op het moment dat het programma werkelijk tot decoderen overgaat. Als je dan ook nog een programmaatje hebt om de code weer in te voegen hoeft elk stuk software dus nog maar 1 keer in zijn bestaan gekocht te worden.
Het hele verhaal roept een paar interessante vragen op. Is het bijvoorbeeld strafbaar om de codes waarmee de programma's zijn versleuteld te verspreiden? Hebben al die bedrijven (waaronder zelfs IBM) wel toestemming om het DES-algoritme uit te voeren uit de Verenigde Staten? Heeft het nog wel zin om software tegen onbevoegd kopiëren te beveiligen?

Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende Ein Organ des Chaos Computer Club

Cryptowet voorlopig van de baan

Wij ontvangen nogal wat electronische post. Van die post is een aanzienlijk deel gecodeerd. De afzenders van die berichten hebben ons iets te melden, maar ze willen liever niet dat de hele wereld weet dat het van hen afkomstig is. Hack-Tic drijft voor een groot deel op de inspanningen van anonieme lezers, ergens diep in de buik van 'het systeem'. Het systeem, de regering, de multinationals, de PTT (oeps: KPN), geef het beestje een naam: ze zouden er met z'n allen een lieve duit voor over hebben om er achter te komen wie onze bronnen zijn.

We waren dan ook op zijn zachtst gezegd mild ontstemd toen we vernamen dat de regering van plan was om, in de nieuwe wet op de telecommunicatievoorzieningen, cryptografie te verbieden. Alleen met een speciale ontheffing mag je nog iets versleutelen, maar dan moet je wel je geheime sleutel bij de staat registreren, en gebruik maken van een geregistreerd algoritme.

Gelukkig waren we niet de enigen die dit scenario niet helemaal zagen zitten. Binnen een paar dagen stonden er artikelen in de kranten en werd er zelfs in het NOS-Journaal over bericht. Nog een week later was de Digitale Burgerrechtenbeweging in oprichting. Ook het VNO en andere werkgeversorganisaties lieten weten niets in de wet te zien. Bien etonné de se trouver ensemble. Columnisten lieten in hun artikelen merken dat ze doorhadden waar het om ging: dit is geen strijd van een paar computernerds tegen de regering, dit is de regering tegen ons allemaal.

Niet veel later kwam het bericht dat de regering afzag van het gewraakte wetsvoorstel. Kennelijk waren ze niet voorbereid op de storm van protest die in zo'n korte tijd de kop had opgestoken. Maar uit de (anonieme, gecodeerde) geruchtenmachine is vernomen dat men van plan is de cryptowet in gewijzigde vorm alsnog in een wet op te nemen. Vooral voor het bedrijfsleven (banken, verzekeringsmaatschappijen) zijn de scherpe kantjes er afgehaald, maar de geest van de wet blijft ongewijzigd. U heeft helemaal geen recht om iets voor destaat geheim te houden!

Alleen al het IDEE dat wij onze geheime sleutel bij de staat zouden inleveren.... Ze komen onze sleutel maar halen, dan mogen ze gelijk duimschroeven meenemen voor de wachtwoorden. En ja, de wet is makkelijk te omzeilen, maar dat geldt voor meer wetten. Wil jij wonen in een land waar je een crimineel bent als je iets voor de staat verborgen houdt?

Een democratie kan alleen functioneren als mensen vrij met elkaar kunnen communiceren. Vrije pers, zoals de makers van de grondwet dat bedoelden, kan alleen vrij zijn als ze kontakt met anonieme bronnen kan hebben. Anonimiteit is in het informatietijdperk alleen door middel van de cryptografie veilig te stellen. Als jullie prijs stellen op dit tijdschrift en/of op jullie burgerrechten dan zullen jullie moeten helpen om te zorgen dat zo'n wet er **nooit** doorkomt. Du haßt es gewüßt!

Rop

Hackers voor de rechter

Op een naargeestige maandagmorgen in januari 1992 heeft het team computercriminaliteit van de gemeentepolitie Amsterdam een primeur: voor het eerst in onze vaderlandse geschiedenis worden er twee personen gearresteerd op verdenking van hacken. Rob (alias Fidelio) en Harry (alias Wave), dan 25 en 21 jaar oud, worden beschuldigd van het hacken van 'bronto.geo.vu.nl', een Unix-systeem van de faculteit der Aardwetenschappen van de Vrije Universiteit van Amsterdam.

Daar dit voorval plaatsvindt in het gezegende tijdperk voor de invoering van de wet Computercriminaliteit, die pas op 1 maart 1993 in werking is getreden, luidt de beschuldiging: valsheid in geschrifte, vernieling en oplichting. De computerapparatuur van de verdachten wordt in beslag genomen en zijzelf worden 9 dagen vastgehouden voor verhoor, waarin zij hun hack bekennen. Vervolgens gaat de ambtelijkjuridische molen aan het draaien en op 3 mei 1994 is het zover: om 9 uur 's morgens moeten Rob & Harry voor de rechter verschijnen om verantwoording af te leggen voor hun daden van ruim twee jaar geleden.

Wanneer uw verslaggever zich op deze historische dag, stipt om 10 minuten over 9, op de klapstoeltjes van de publieke tribune van de rechtbank aan de Amsterdamse Parnassusweg laat zakken, is de aktie in de zaal reeds begonnen. In de zaal bevinden zich drie rechters, een griffier, de officier van Justitie en de twee verdachten, die worden bijgestaan door twee advokaten. Beneden op de tribune zitten een handjevol journalisten en enkele wetsvertegenwoordigers. Wij ontwaren tenminste dhr Koomen, hoofd van het team computercriminaliteit van de Amsterdamse politie en een vertegenwoordigster van de Centrale Recherche Informatiedienst. Op de publieke tribune, die als een balkon boven de zaal hangt, zitten een stuk of 15 *Timewasters** en andersoortige hackers gespannen naar beneden te turen.

Een van de advokaten heeft het woord. Zij meent dat justitie na de arrestatie van Rob en Harry dermate lang heeft gewacht met het voor de rechter brengen van de zaak, dat de grenzen der redelijkheid zijn overschreden. Zij wijst er op dat de Hoge Raad reeds enige jaren geleden heeft bepaald dat de 'redelijke termijn', die tussen aanhouding en rechtszaak in acht genomen dient te worden, maximaal 2 jaar kan bedragen. Die termijn zou in deze zaak met een maand zijn overschreden. Omdat het Openbaar Ministerie niet aannemelijk kan maken dat een langere termijn noodzakelijk was voor het onderzoek, maar eerder de indruk wekt al die tijd te hebben stilgezeten, vraagt zij de rechters het Openbaar Ministerie niet ontvankelijk te verklaren. Dat zou betekenen dat er geen rechtszaak plaats zou vinden.

De Officier van Jusitie, die vervolgens het woord krijgt, hangt de mening aan dat het OM zich nog net aan de redelijke termijn heeft gehouden. Ter illustratie begint hij eveneens op omstandige wijze met data te gooien en komt op een eindresultaat van precies 24 maanden. Daarnaast verweert hij zich tegen de aantijging dat het Openbaar Ministerie zou hebben zitten slapen in de tussenliggende tijd. Het OM heeft



maar liefst twee deskundigen aangewezen die moesten uitzoeken wat Rob en Harry nu precies misdreven hadden. De eerste deskundige geeft, na enkele maanden van stilzwijgen, zonder duidelijke redenen plotsklaps de opdracht terug. De tweede deskundige, die als 'opvolger' wordt aangewezen, hanteert eenzelfde strategie. Het OM heeft dus wel duidelijk aktiviteiten ondernomen. Zij het met wat weinig resultaat, want een deskundigenrapport is er dus nooit gekomen.
Dit alles minzaam aangehoord hebbend schorst de president van de rechtbank de zitting voor twintig minuten. Na ongeveer een uur, waarin op de publieke tribune druk wordt gespekuleerd over de afloop van de zaak ('ik hoop maar dat het OM niet ontvankelijk wordt verklaard' - 'ja, maar dan zijn we wel voor niets zo vroeg opgestaan' - doe niet zo egoistisch, joh! stel je voor dat jij daar zat!' - 'nee hoor ik meen het ook niet echt') schrijdt de rechterlijke macht de zaal weer binnen.
Wanneer iedereen zich weer geïnstalleerd heeft, neemt de president van de rechtbank het woord. De zaal hangt muisstil aan haar lippen. De rechtbank gaat mee in de rekensom van de Officier van Justitie, en meent dat de redelijke termijn tussen aanhouding en zitting niet overschreden is. Hoewel de twee jaar dus redelijk wordt geacht, vindt de rechtbank het toch een erg lange tijd. De verdachten zijn nog nooit eerder met justitie in aanraking geweest en zij hebben al die tijd doorgebracht met de dreiging van een rechtszaak, als een donderwolk boven hun hoofd. De carrière van een van hen heeft daar reeds schade van ondervonden en de toekomstige carrière van de ander zou er door geschaad kunnen worden. Daarnaast blijkt, uit de tapverslagen van afgeluisterde telefoongesprekken tussen de verdachten, dat zij zich ten tijde van hun hack er niet bewust van waren dat zij een strafbaar feit begingen. Zij bespraken onder andere telefonisch de op stapel staande wet Computercriminaliteit met elkaar en konstateerden dat wat zij nu deden over een jaar verboden zou worden. Dit alles in overweging genomen besluit de rechtbank dat het belang van de verdachten zwaarder weegt dan het belang van het Openbaar Ministerie en verklaart daarom het Openbaar Ministerie, conform de eis van de advokaat, niet ontvankelijk.
Een zucht van verlichting gaat door de zaal, de Officier van Justitie loopt rood aan en applaus stijgt op van de publieke tribune. De eerste rechtszaak tegen Nederlandse hackers is toekomst geworden.

Hanneke

*Timewasters, een groep hackers waarvan het epicentrum rond de TU Eindhoven ligt

Hulde! (tuig)

In de vorige Hack-Tic plaatsten we onder de kop 'Schrijven Tuig!' een welhaast wanhopige oproep om meer lezerspost in te zenden. We riskeerden zelfs een faillissement door voor iedere geplaatste brief een abonnement van 10 nummers kado te doen.
Een enkele zeurpiet liet ons weten dat hij niet met 'tuig' aangesproken wilde worden, maar een hoop andere mensen doken nijver achter hun tekstverwerker (we krijgen hier alleen heel zo nu en dan nog wel eens een handgeschreven brief). Maarliefst 13 pagina's kunnen we nu met lezersbijdragen vullen. We handhaven ook voor het volgende nummer ons aanbod, tot we allemaal op straat moeten bedelen om de volgende Hack-Tic nog te kunnen versturen.
Geen dossier zo geheim, geen corporate-image zo onkreukbaar, geen systeem zo 'onkraakbaar' of er is ergens een Hack-Tic lezer die er iets over te melden heeft.

Begraaf ons in stapels post, e-mail en faxen

Beste Hack-Tic,

Na bestudering van het batchfiletje van Valentijn in HT20-21 was ik ervan overtuigd dat het kleiner en sneller kon. Het resultaat van 'vele nutteloze uren plezier' zien jullie hieronder.
In plaats van +r maakt ik gebruik van -a, want dat merkt het slachtoffer namelijk minder snel. Het XCOPY commando maakt het mogelijk selectief .bat files te kopieëren, verder speekt BatVirus voor zichzelf.
P.S. Wie kan dit beter

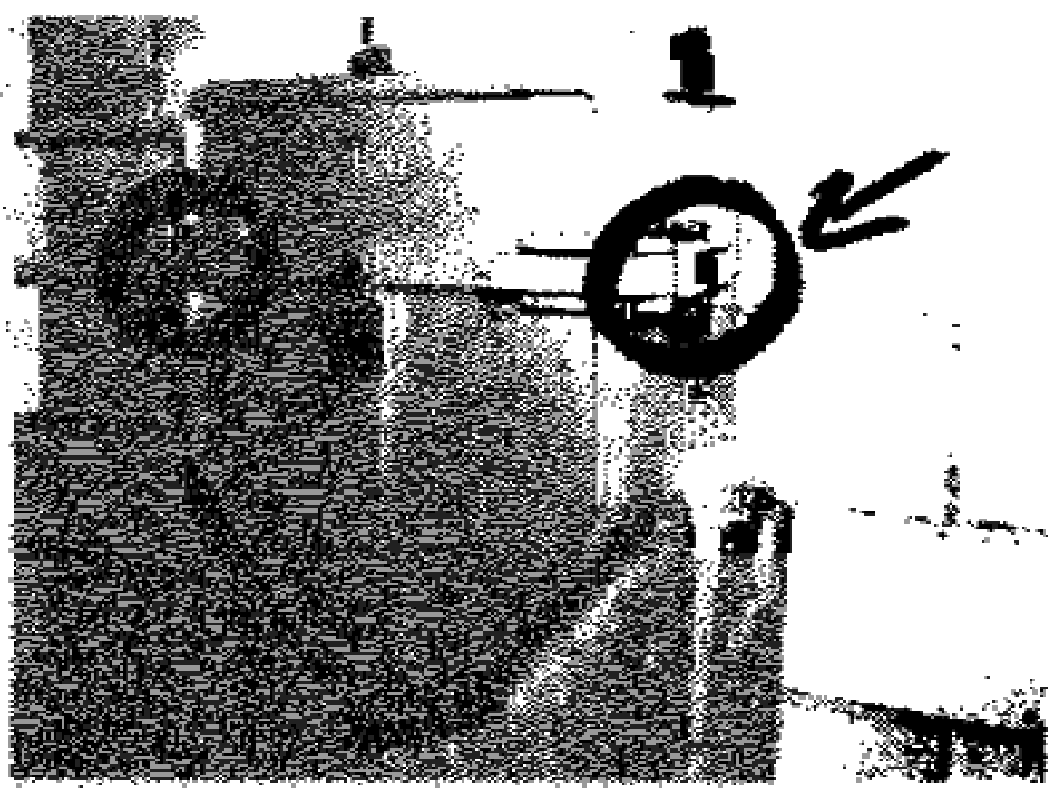
Jaap

```
ctty nul
md v
attrib -a bv.*
xcopy *.bat v\ /a
copy v\*.bat v\*.b
for %%a in (v\*.bat) do copy bv.* %%a
copy v\*.bat + v\*.b *.bat > nul
deltree /y v
attrib -a *.bat
```

Not bad indeed, maar de 'gebruiker' moet wel DOS6 hebben, want anders heeft hij/zij deltree niet, en dan blijven overal directories hangen.

Geachte Ptt,

Waar blijft al het geld van die eeuwige tariefsverhogingen? U zegt iedere keer dat is om te investeren in de toekomst. Er wordt geschermd met termen als infrastructuur en concurrentiepositie (jullie hebben een praktisch monopolie, want ik kan geen aansluiting krijgen van France Telecom of zo). Ik betaal veel geld voor mijn telefoonaansluiting en ga er van uit dat die afdoende tegen kwaadwillende cyberpunks en technoanarchisten is beveiligd. Voor het bedrag wat u nu weer extra gaat vangen, kunt u naast iedere schakelkast een tot de tanden bewapende Rambo(tm) zetten om die kast te beschermen tegen perverse geesten.



Wat is de realiteit? Geen Rambo(tm) nee. Een stevig hangslot aan een voor de rest zeer FLEXIBELE constructie. Hangslot blijft dicht, kast toch open. Nu zie ik allemaal draadjes en een tabel die me vertelt welke draadjes van mij zijn en welke van die nare buurman. Ik heb slechts één aansluiting en dus in het vier-aderige snoertje nog twee vrij (=gratis bellen). U ruikt het al: de gewone man bij mij in de straat betaalt de updates voor mijn GUS software, die ik uit Canada haal.

Dit is geen ernstig geval. De buurman is namelijk niet aardig. Maar stelt u zich eens voor dat ik louter aardige mensen in de straat had wonen? Ik neem aan dat u slecht slaapt bij het idee dat deze rekeningen door een oud omaatje met slechts AOW moesten worden betaald. Wat heeft u toch een groot hart! Dit onrecht moet een halt worden toegeroepen! Ik stel voor dat het lokaal tarief weer 1 tik per gesprek wordt of dat alle sysops, cyberpunks en inbellijnen van mainframes via het nieuwe, nog niet operationele, digitale autotelefoonnetwerk van AT&T gaan werken.

Twee arme, digitale studenten.

De PTT zegt zelf dat het telefoonnet adequaat beveiligd is en dat misbruik van andermans lijn bijna is uitgesloten. Mensen met hoge rekeningen moeten gewoon betalen. Het betreft hier dus een waanvoorstelling: zo makkelijk kan het toch niet zijn? Zo makkelijk is het dus wel, en het bellen op rekening van de buurman is daardoor een totale rage geworden. In gebieden met veel hoogbouw is de PTT als een tamme idioot bezig om draden door stalen pijpen buitenom te laten lopen. Maar krijg beslist niet het idee dat er iets aan de hand is hoor....
Is Internet wellicht een beter idee om je software goedkoop te updaten?

Lieve Hack-Tic,

Kwartjesvenster telefoon

Onlangs kwam ik weer zo'n oude telefoon met kwartjesvenster tegen, dus ik pak mijn piepdoosje en bel een exotisch nummer. En wat een geluk de toontjes worden toegelaten, echter blijkt de telefoon honger te hebben en begint om kwartjes te zeuren. Hoe kan dat? En hoe kan ik dit voorkomen? Ik heb vaker met dit soort telefoons gespeeld en jawel in 1994 zijn er nog steeds die werken, uiterst zeldzaam maar toch.
In de Telegraf stond een artikel over het zoveelste fraudegevoelige PTT-toestel. Het gaat hier om het type Matterhorn dat op de markt wordt gebracht onder de naam Coinvox 10. Weten jullie die truuk, is dat soms hetzelfde als met het kwartjesvenster?

Blue-Boxing

Ook uiterst zeldzaam zijn telefoonnummers om mee te blueboxen. Na drie pleisters op mijn vingers heb ik er enkele gevonden.
[heel verhaal wat er op neerkomt dat het niet lukt met de bluebox]
Hoe zit dat met die Frank R2 (wellicht vernoemd naar het internationale signalerings-systeem R2) die in de pers kwam omdat hij via/vanuit Belgie kon bellen en de rekening bij iemand anders kon laten belanden? Gebruikt hij een bluebox?
Hij maakt gebruik van het R2 signaleringssysteem (overigens een nationaal systeem, de R staat voor Regional). Hij gebruikte daarvoor op de demonstratie op Hacking at the End of the Universe een Demon-Dialer. In Belgie kun je dan de ANI vervalsen, waardoor hij een willekeurig nummer op het scherm van de operator kan toveren. Zo kan hij dus handmatig bemiddelde gesprekken op rekening van een ander zetten. Het systeem R2 is overigens wel tricky, omdat je de terugkomende signalen moet interpreteren, het is een full-duplex protocol.

Lock-Picking

Ik heb onlangs maar eens een slot van de telefoon uit een telefooncel geoogst. Sleutels bleken zonder certificaat niet te krijgen, en ook lockpicken ging niet, dus zette ik de boor er maar in. Het slot blijkt helemaal vol te zitten met mushrooms, spools, kogeltjes en andere ellende. Misschien interessant voor de heer The Key (of de trunk junks uit Hack-Tic 3).

NS-telefoons

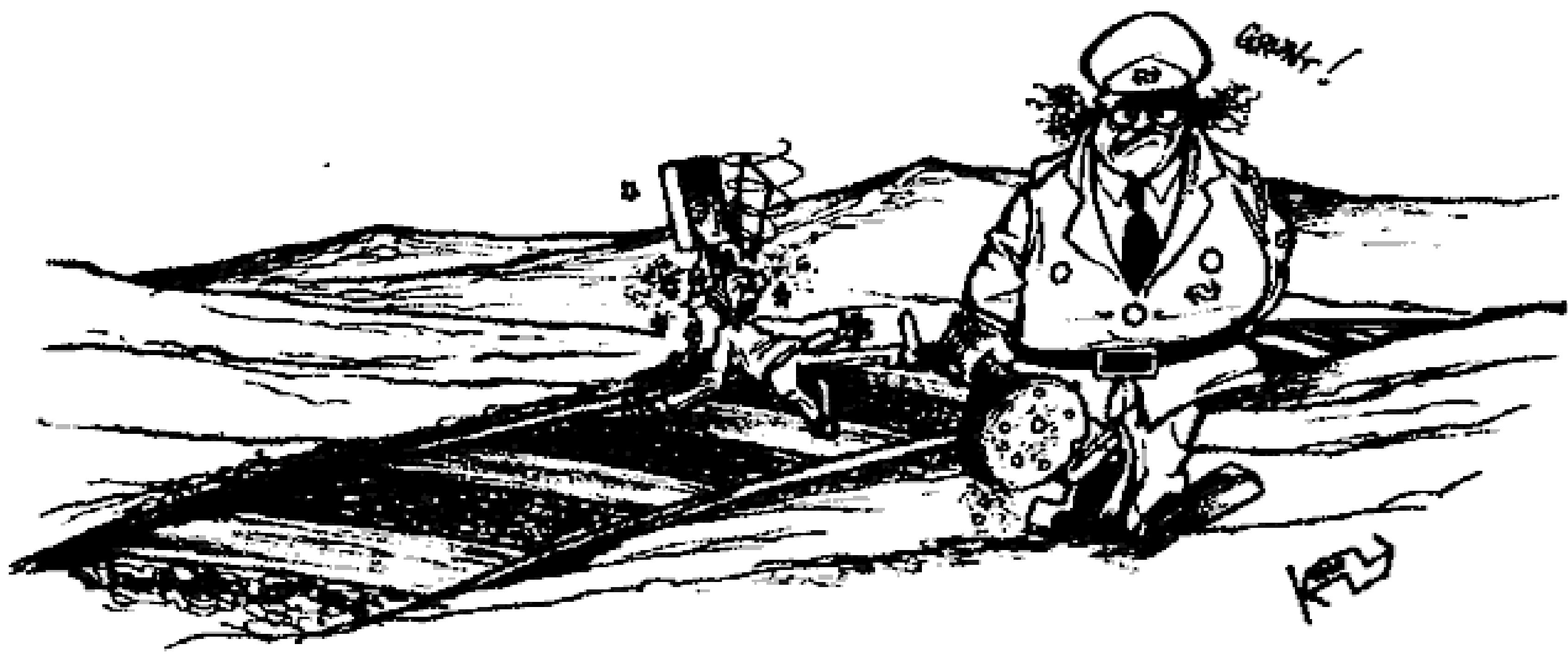
De telefoonkastjes van de NS, van die kleine grijze kastjes met een grote zwarte bel erboven. Op het kastje staat de naam Ericsson. Met een vierkante sleutel (of een punttangetje) simpel open te maken. Je kunt met de telefoon die er in hangt gewoon bellen als je eerst een nul kiest, alleen internationale en 06-gesprekken zijn geblokkeerd. Als ik me niet vergis bevindt het zenuwcentrum zich in Utrecht, dus het zou best kunnen dat al deze verbindingen vanuit Utrecht het telefoonnet op gaan.
Je hoeft mij ook niet te vertellen dat zo'n NS telefoon geen comfort heeft, het kan buiten inderdaad koud zijn of zelfs regenen. Maar je moet er iets voor over hebben om gratis te bellen, en zo gebruik je je Openbaar Veevervoerkaart ook nog eens nuttig.

GSM

De informatie uit Hack-Tic over ATF-1 en semafonie heb ik goed kunnen gebruiken voor mijn stageverslag, ik had zowaar een negen.Ik heb overigens het een en ander meegestuurd over het ONKRAAKBARE GSM. Niet helemaal voor mij weggelegd, maar wie weet kunnen jullie er iets mee.

Listerique

Bij het artikel over kwartjesvenstertelefoons (lang geleden!) stond ook dat het niet in alle gevallen werkte. Verder zijn telefoons die al te veel verlies voor hun eigenaars opleverden inmiddels door natuurlijke selectie vervangen. Survival of the fittest. Zie ook het stukje over de nieuwe 008-truuk in deze Hack-Tic.
Wat betreft dat Telegraaf artikel: Het gerucht wil dat als je twee stuivers tegen elkaar aanhoudt en inwerpt, het toestel denkt dat je een munt van vijf hebt ingeworpen. Wij hebben het zelf niet geprobeerd, maar het klinkt dermate stupide dat het waar zou kunnen zijn. Proberen.....
Blueboxing is helemaal zo makkelijk niet meer. Sterker nog: we kennen zelf nog maar twee of drie mensen die echt zelf nieuwe dingen kunnen ontdekken. Als middel om gratis te bellen is de bluebox nagenoeg dood, als experimenteerdoos zijn er nog wel mogelijkheden. De PTT is er trouwens tegenwoordig veel sneller bij om nieuwe gaten te dichten, maar anders zou het geen uitdaging meer zijn.]
The Key heeft zelf (overigens geheel legaal) ook wel eens naar zo'n slot van een telefooncel gekeken. Zijn conclusie was ook dat de staalboor het enige middel was om het slot zonder sleutel open te krijgen. Hebben ze ook eens iets goed beveiligd, ere wie ere toekomt.
We denken dat de vriendelijke heren van de spoorwegpolitie je eerst in elkaar knuppelen en dan wel eens uitzoeken wat je met die diensttelefoon aan het doen was. En dat voor een gewoon interlokaal gesprek. Erg wanhopig hoor.
GSM heeft (zeker vanwege PTT-claims over afluisterveiligheid) onze warme aandacht. Wie weet in een volgende Hack-Tic....



Beste Hack-Tic

Correctie kostenteller

Gaarne maak ik gebruik van de mogelijkheid een mailtje naar de redactie te sturen en wel om de volgende reden. In HackTic 8, uit een ver verleden maar gelukkig herdrukt voor de HCC-beurs en dus in ieders bezit, presenteerde BILLSF een zelfbouw-kostenteller. Een ingenieus ontwerpje dat zo goed telt dat op diverse centrales ook het belsignaal ('wektoon') onderdeel wordt van de telefoonrekening. Hoe kan zo'n blunder toch in vredesnaam in een gerespecteerd blad als het uwe terechtkomen?
Wat is het geval? BILLSF merkt ten onrechte op dat de aarde altijd tussen A en B inhangt - qua spanning. Neen, driewerf neen, veel vaker hangt de B in rust zo'n beetje aan aarde en A voert dan -50V.
Wanneer iemand belt komt A aan aarde te hangen, B voert -50V. De belspanning staat soms op beide draden (de aarde hangt dan keurig in het midden), maar net zo vaak op1 draad: het gemiddelde komt in dat geval ruim boven de 15 volt, in extreme gevallen zelfs op een volt of 35 (uitgaande van 90Veff belspanning; {2*90=127). In het geval de wektoon op1 draad staat, komt de spanning op de basis van de BC546 op een ruime 1,6 volt te staan. Need I say more?
Stel nu, dat ook de kostenpuls het een beetje laat afweten. Er staat bijvoorbeeld niet precies twee maal honderd volt gesuperponeerd op de normale spanning, maar, laten we zeggen, twee maal 60 volt. Het resultaat op de basis is een spanning van 1,8V. Het wordt nu dringen voor de poorten van de 74HC00. En spannend voor de ontwerper! Zal hij de gevoeligheid van zijn schakeling zover doen afnemen dat deze nergens meer op reageert? Of zorgt hij ervoor dat hij middels een ferme diode in de buitenlijn de telefoon eerder opneemt dan de bel de kassa doet rinkelen?
Enfin, dit geintje (met bijbehorende 2 x 60V) heeft mij behoorlijk wat hoofdbrekens gekost. Uiteindelijk heb ik 't eenvoudig opgelost met een tweede transistor. Uitgaande van het feit dat zowel a als b enkel tijdens een kostenpuls beiden positief zijn, kan met behulp van twee transistortjes en een AND een prachtige teller worden gemaakt. Zelf heb ik tweemaal een BC546 gebruikt, twee weerstandsdelers (1M/82K) en de in jullie schema gebruikte HC00 (waarvan de extra NAND voor som van de signalen. De transistoren hangen uiteraard van + naar ingang, met een 47K naar aarde.
Voor de teller heb ik ooit eens rekenmachientjes gebruikt. We hadden in die tijd nogal wat atoomoorlogen en dat deed de teller op bizarre waarden springen. Nadat de teller tot drie keer toe pi in 30 decimalen had vertoond, kocht ik bij een dumpzaak enkele 6 volt mechanische tellers. Met een magneetje. Hebben de Zondvloed al overleefd, de inquisitie, het vernietigen van de aarde wegens interstellaire highway en een knokploeg wegens huurachterstand. Staan nooit zomaar op pi. Trekken 54mA. Voor F1,75 en dat is minder dan 30 cent per volt. Vind daar maar eens een apparaat voor tegenwoordig! Dit alles via een extra BC548 voor de noodzakelijke stroom.
Hopende op een reactie, met Dank en Bewondering voor uw tijdschrift/ mijn lijfblad,

Valentijn

Kostenpulsen zijn inmiddels een 16KHz toon. Zie het artikel daarover in deze Tic.

Hallo Hack-Tic,

Rara, wat gebeurde er vannacht?

om 23:58 had ik verbinding met Mexico; dus leg ik snel de hoorn op de haak want de tikkenteller begon te lopen. En rara: de tikker liep door! (5.85 / min!). Uitstekkeren van m'n gehele systeem had niet het gewenste resultaat: geen kiestoon bij het herinschakelen en een als de nete tikkende teller...
De storingsdienst, die natuurlijk vanuit een cel gebeld moest worden waarvan de guldengleuf potdicht zat en mij dus 4 guldens heeft gekost, kon mij slechts geruststellen: maandagochtend wordt de klacht verholpen, en zondagnacht zal de tikker gewoon blijven doorlopen...
Bijna 20.000 tikken verder... hield vanochtend de tikker op en werd de storing verholpen. Nu maar hopen dat de rekening niet "buitensporig hoog" is, want dan moet ik nog even 060404 bellen...

Bob

Hebben wij ook wel eens gehad, op Hacking at the End of the Universe. Was jij dat soms?

Waarde redactie,

In HT20/21 leverde ik de mensheid een verbeterd batchvirus en ik haast mij te zeggen dat dit nog niets aan kracht heeft ingeboet want ik ben het in geen enkele viruslijst tegengekomen!
Ondertussen staat de concurrentie niet stil. Ik zag onlangs een virus dat in een zeer hoge programmeertaal geschreven was, namelijk de menselijke:
"This is a signature virus! Copy me into your own signature!"
Er verschijnt elke maand wel een besturingssysteem dat nog trager is dan het vorige en ik heb berekend dat vanaf medio juni VVIRUS langzamer werkt dan TICVIRUS op de oorspronkelijke 386/33. Daar moest ik wat aan doen!
Indien u deze file als een .bat hebt opgestart, bent u inmiddels meervoudig eigenaar van de nieuwste versie van VVIRUS, namelijk VVIRUS 5.1. Korter en sneller!
En nu we het toch over WordPerfect hebben: de WP6 makrotaal werkt met textbestanden met commando's. Kan de Hack-Tic weer eens een ouderwetse appeltaart uitloven voor de eerste WP-virus-makro? (Ik heb zelf een XT en kan derhalve geen diensten bewijzen).
Ik wens u en root vele uren plezier met het respectievelijk verzinnen en uitvoeren van toepassingen van deze batch.

Valentijn

Jullie hebben het gelezen: virussen in WP-macros voor de volgende Tic. Geen appeltaart, wel een abonnement voor de schrijver (of schrijfster) van een geplaatste brief. Het batchvirus staat op de volgende pagina.

```
@ctty nul
@copy *.bat *.ba
@type %0.bat|find " @">_._
@for %%a in (*.ba) do copy _._+%%a %%at
@del *.ba
@del _._
@attrib +r *.bat
@ctty con
```

Misdaadanalyse

Een lezer stuurt ons een lijstje met ernstige vergrijpen, begaan in het rekencentrum van de Noordelijke Hogeschool Leeuwarden. Hier worden ondermeer de vooroordelen bevestigd dat computertypes niet kunnen spellen (Jaja, er hebben in Hack-Tic ook zo hier en daar wel een paar spelfoutjes gestaan) en dat systeembeheerders geen gevoel voor humor hebben. Prettig om in zo'n situatie kennis op te doen. We hadden gelukkig toch al niet zo'n hoge pet op van 'georganiseerd onderwijs'. Sabotage, it's as simple as pulling the plug.

- Opdrukken van GIF-bestand op RC2
- Het bij zich hebben van software andere dan die voor het prakticum gebruikt moet worden.
- Listing van programma's uitgedraaid en in bezit van het RC.
- Aanmaken van een login-look a like alsmede het knoeien in autoexec.bat dit kan alleen maar via lagere dos-utility-tools gedaan worden.
- Draait pak papier uit op de seikosha printer met daarop allerlei onzin (humorlijst.... ook een soort lijst via mail)
- Onklaar maken van apparatuur door eigen floppies.
- Tijdens prakticum van Ponne aan het spelen
- Eten, geen collegekaart
- Command.com gewist
- Verwijderen van /3open/lanman gewist. Deze gebruiker was de laatst ingelogde persoon.
- Prime-misbruik met het sturen van messages aan personen wie dat niet wil. (g. van der Kooij)
- Heeft hoofdschakelaar van pc uitgezet terwijl er nog gebruikers bezig waren Meule023. Gevraagd om excuusbrief te schrijven aan Meule023 en collegekaart te tonen. File van meule023 was verminkt.
- Koffie, Geen collegekaart
- Op lokale C-schijf geprutst
- Copieren van bestanden van de lokale C-schijf naar onder andere D Tevens had hij de beide virtuele schijven losgelaten.
- Het vervuilen van gebruikers met onzinnige mail en tevens het vragen van donaties voor iets welke NIET zijn eigendom is.
- Is alleen maar toegestaan als UNIX gebruiker.
- Wijzigen van command.com en autoexec.bat. Directe gevolg : Letters op de kop.
- Command.com gewist

NECRONOMICON

TEKST & TEKENINGEN
KOEN HOTTENTOT

'Necronomicon' is het eerste stripboek van Hack-Tic's hoftekenaar Koen 'KoHo' Hottentot. Lees over God die een pilsje pakt in de hel, en over de ware betekenis van steencirkels. Over een dodelijke bingo-avond, een mislukt zelfmoordenaar, illegaal gedestilleerde hopjesvla, een gerecyclede maaltijd en een gruwelijk mislukte goocheltruuk. Om nog maar te zwijgen van de waarheid omtrent de dood van John F. Kennedy, van schipbreukelingen die vies van elkaar zijn en van Adolf Hitler die in een gevangenis in Arizona verdwijnt - en nog veel meer.
'Necronomicon is gedrukt in een oplage van 500 exemplaren, allen door de auteur handgeprijsd. Door overmaking van fl. 5,99 + fl. 2,80 porto kunt u de gelukkige eigenaar worden van dit stripboek. Zeker wanneer u dat doet op het juiste bankrekeningnummer: 37.01.53.510 t.n.v. K. Hottentot, Koog a/d Zaan.
Maar wat draalt u nog !? Bestel !!!



Hack-Tic Kostenteller Nieuwe Stijl

De PTT heeft de oude kostenpulsen (50 HZ, 50 Volt tussen de gesprekslijnen enerzijds en de aarde anderzijds) onlangs vervangen door een toon van 16 KHz die net als de audio van het gesprek als wisselspanning op de gesprekslijnen staat. Voorlopig bestaat de kostenpuls op de meeste plaatsen uit de twee signalen tegelijkertijd, maar de oude kostenpuls zal in de toekomst verdwijnen.
Hier een schema om zelf iets te laten schakelen door de kostenpuls nieuwe stijl, veel leuker dan dure spullen kopen van de PTT of anderen. Je kunt aan de andere kant van het relais bijvoorbeeld de '=' toets van een rekenmachientje hangen, maar dat idee gaven we je ook al in Hack-Tic 8. Niet iedere lijn heeft kostenpulsen, daar moet je bij de PTT voor betalen. Alsof je bij de supermarkt extra moet betalen voor de prijsjes op de pakken....
Kostentikken krijgen is met deze schakeling een waar genot, alleen gratis bellen is natuurlijk nog leuker.

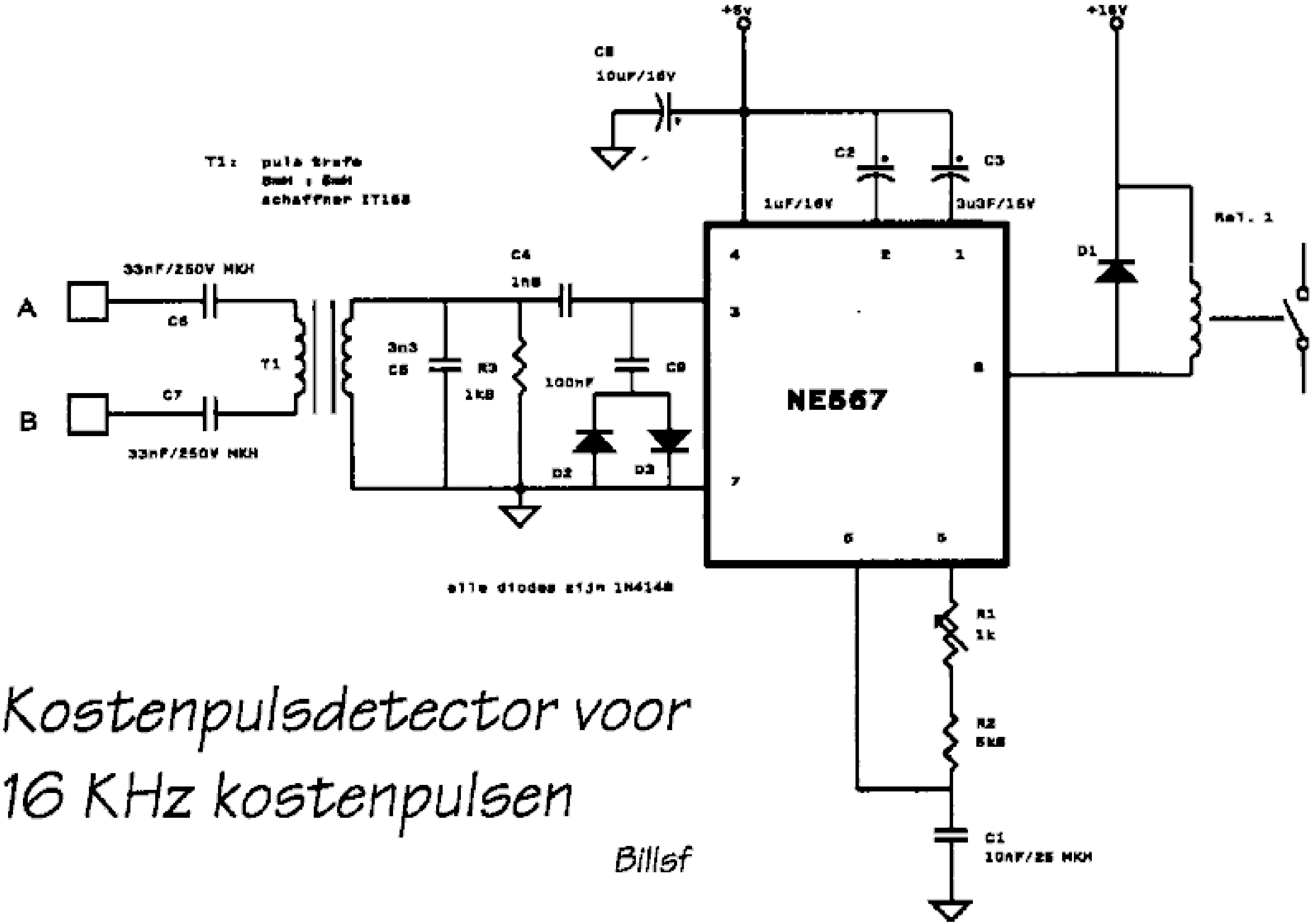
Hoe werkt het?

C5, C6, C7, T1 en R3 vormen samen een afstemkring die resoneert op 16 KHz. De 567 is een 'phase-locked-loop tone-decoder' die door middel van R1, R2 en C1 is afgesteld op 16 KHz. De 567 brengt pin 8 naar een logisch laag nivo op het moment dat op pin 3 een 16 KHz toon (de kostenpuls komt te staan. Pin 8 kan 100 mA trekken, dus een klein relais is daarmee wel aan te sturen. De diode over het relais is alleen nodig als er ook echt sprake is van een relais, en dient om de chip tegen 'terugslag' van de spoel van het relais te beschermen.

Onderdelen

Voor C1, C5, C6 en C7 heb je condensatoren van goede kwaliteit nodig, liefst foliecondensatoren (5% tolerantie of beter). C2, C3 en C8 zijn doodgewone elco's en de rest maakt helemaal geen fluit uit.
De potmeter R1 dient om het geheel af te stemmen op 16 KHz. De makkelijkste methode: bellen naar iets dat achterlijk veel geld kost en dan draaien tot het apparaat kostentikken begint te zien, vervolgens doordraaien tot ie ze niet meer ziet en dan terugdraaien tot ergens midden in het zojuist gevonden gebied. Let op: als je apparaat niet binnen 30 seconden op kostentikken reageert dan is er waarschijnlijk iets anders mis, het heeft geen zin om de PTT onnodig te spekken. Je kunt natuurlijk ook een 16KHz toontje ergens vandaan toveren (toongenerator of zoiets).

Billsf



Kostenpulsdetector voor 16 KHz kostenpulsen

Billsf

KPN-Goldcard

Chipkaarten hacken niet eens een echte uitdaging

Oh nationale trots, beste belegging sinds OGEM, ultieme winstenmaker en tarievenverhoger. Uw naam is heilig. Uw geldzucht is voor telecommunicatiebedrijven wereldwijd een lichtend voorbeeld. In Uw aanschijn zullen zij afrekenen met de laatste restjes van maatschappelijke betrokkenheid binnen hun organisatie.

Maar eh.... Die nieuwe telefoon-chipcard van U. Die is een beetje te dom.

Je hebt ze wel gezien: prachtige kaarttelefoons van het merk Landis & Gyr die alle types kaarten aannemen. Ze slikken de oude optische telefoonkaarten, de nieuwe chipcards, en allerlei magneetkaarten. Over de optische kaart hebben we in het verleden al het een en ander gepubliceerd, en ook magneetkaarten zijn in Hack-Tic al uitgebreid aan de orde geweest. In dit artikel lees je hoe de telefoon-chipcards werken en hoe iedereen ze zelf kan uitlezen, beschrijven en ... nadoen.

Eerst maar eens uitleggen hoe het werkt. Er zijn op het moment in de wereld twee soorten 'prepaid' telefoonchipcards te onderscheiden.

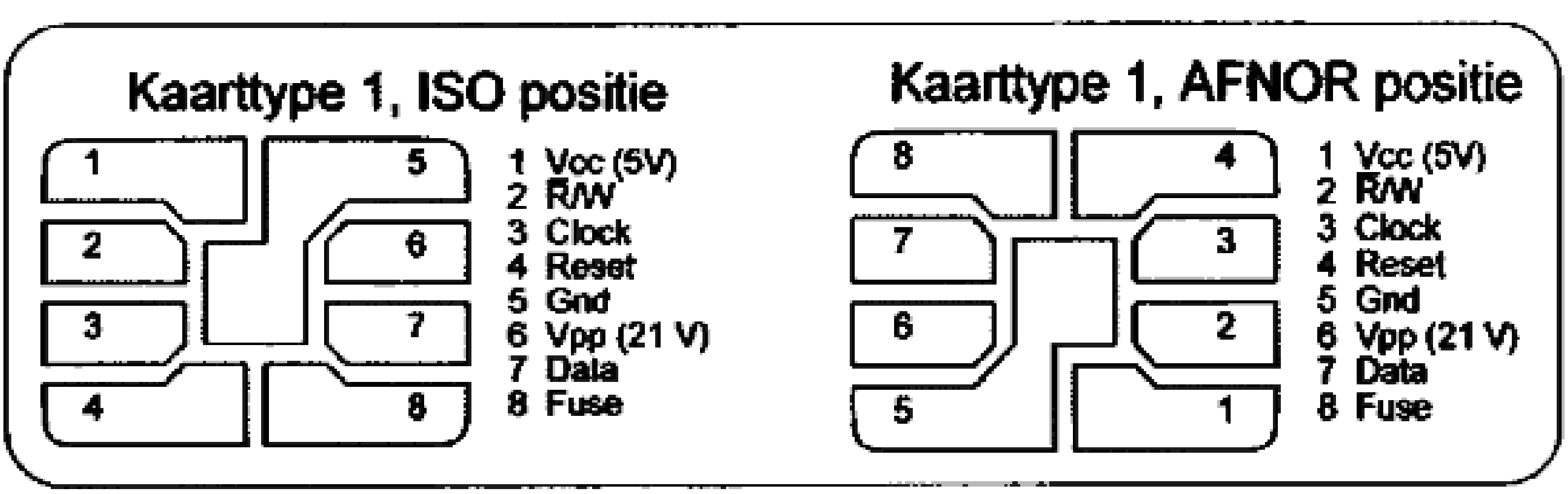
Kaarttype 1

De oudste van de twee is een kaart die o.a. door de firma's Gemplus, Solaic, Schlumberger en Oberthur wordt gemaakt. Dit type kaart heeft twee varianten, de ene variant is in gebruik in Frankrijk en Monaco, en de andere in Zweden, Spanje, Noorwegen, Andorra, Ierland, Portugal, Tsjechie, Gabon en Finland.

De kaarten werken met synchroon protocol en zijn gebouwd met N-MOS techniek. Ze bevatten een 256 bit EPROM, waarvan 96 bits 'write-protected' zijn met een zekering die wordt doorgebrand. De chip gebruikt 85 mW als ie gelezen wordt, heeft 21 Volt nodig om geprogrammeerd te worden en heeft een access time van 500 ns.

Chip-positie

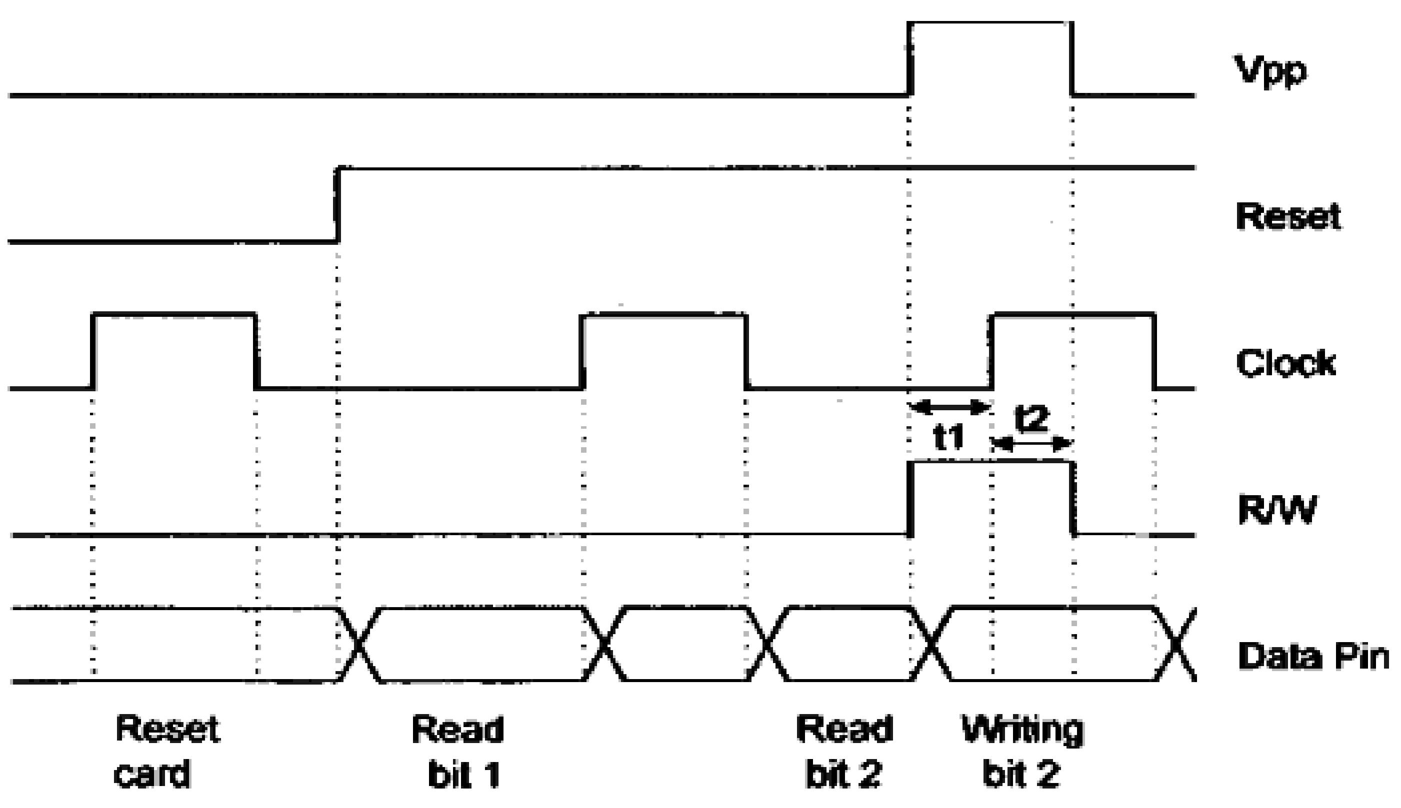
Allereerst de positie van de chip op de kaart, de chip kan namelijk op twee plaatsen zitten. De eerste positie wordt



soms AFNOR genoemd. De oude franse chips zaten op die plek op de kaart. De nieuwe positie is een ISO (International Standards Organisation) norm, en ook de Fransen zijn inmiddels overgeschakeld naar de ISO-positie. Als je zelf een reader/writer gaat bouwen (daarover straks meer) dan heb je waarschijnlijk genoeg aan een chipcard-adapter die alleen de ISO-positie heeft, de Franse positie sterft snel uit.
Op de tekeningetjes op de pagina hiernaast zie je de pin-outs van de chips op AFNOR en ISO-kaarten. De kaarten liggen in de tekening met de chipcontacten naar boven en de chip links. Als je wilt weten waar de ISO-chip zit dan koop je maar even een telefoonkaart.

Werking

Op de volgende tekening zie je een timing-diagram, waarop je kunt zien wat de verschillende signalen doen. Er staat het volgende: als je reset laag maakt en je geeft een clock puls dan reset je de teller in de kaart. Als je vervolgens reset hoog maakt dan kun je met clock de bitjes een voor een voorbij laten komen op de output. Als je not-read/write hoog maakt en de programmeerspanning op Vpp zet en vervolgens een clock geeft dan programmeer je het bit waar je met clock heengesprongen was. Dit bit gaat dan van 1 naar 0.
Een paar dingen om op te letten: alle signalen behalve Vpp in de tekening zijn TTL-nivo (laag is nul volt, hoog is vijf volt). De kaarten van dit type waarmee wij getest hebben bleven echter op de 3.3 volt van een notebook-printerpoort ook nog lopen. De input pennen Reset, Clock en R/W kunnen direct op de printerpoort van een PC worden aangesloten. De Vpp wordt geschakeld tussen 5 volt en 21 V. De tijden t1 en t2 uit de tekening moeten allebei tussen de 10 en 50 ms liggen. Als je de kaart uitleest moeten Vpp en Fuse op 5 Volt liggen.
Op de tekeningen zie je de geheugeninhoud van de twee varianten van kaarttype 1.



Veiligheid

De chip op de kaart laat het in de normale interactie via de connector niet toe dat je bits weer terug op nul schrijft, dus ophogen van de waarde van de chipkaart is op het eerste gezicht niet mogelijk. Aangezien de hele chip een EPROM is kun je natuurlijk wel de hele chip wissen met UV-licht. Dit wordt moeilijk, want de chip ligt in epoxy dat geen UV doorlaat. Lukt het je toch dan zul je de eerste 96 bits (landcode, hoe veel eenheden op de kaart, etc. etc.) weer terug moeten schrijven. Dit wordt ook lastig, want er is een hardware-fuse doorgebrand waardoor deze bits na fabricage niet meer geschreven kunnen worden. Conclusie: ophogen van lege kaarten wordt niet makkelijk.

Memory Map kaarttype 1, Frankrijk [illegible]

byte	bits	betekenis
1	0-7	issuer code
2	8-15	$03: Frankrijk / Monaco
3-11	16-87	9 bytes door de fabrikant in te vullen. Bijvoorbeeld fabriek, batch, en misschien zelfs serienummer.
12	88-95	Totaal aantal units x 10 + 10
13-31	96-247	De telefoontikken. Elke keer als een unit verbruikt is wordt een bit in dit gebied naar de waarde "1" geschreven De eerste 10 units worden al in de fabriek geschreven om de kaart te testen. Kaarten zijn 40, 50 of 120 units. Byte 12 is BCD gecodeerd, er staat dus $13 voor 120 units, $06 voor 50 units of $05 voor 40 units. Alle bits die op nul staan in dit gebied vertegenwoordigen een unit. Een tikje simpel, nietwaar?
32	248-255	$FF als de kaart vol is

Memory Map kaarttype 1, andere landen

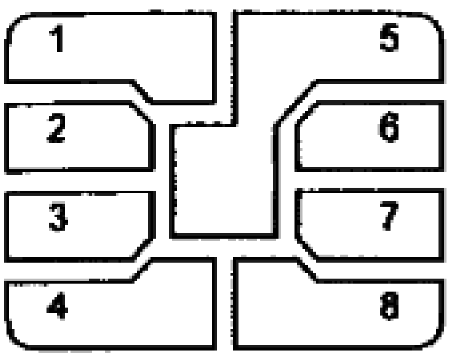
byte	bits	betekenis
1	0-7	issuer code
2	8-15	$83: telefoonkaart van dit type
3-4	16-31	$8XXX: totaal aantal units op kaart plus twee (zie onder)
5-11	32-87	7 bytes door de fabrikant in te vullen. Bijvoorbeeld fabriek, batch, en misschien zelfs serienummer.
12	88-95	Landencode (zie onder)
13-31	96-247	De telefoontikken. Elke keer als een unit verbruikt is wordt een bit in dit gebied op waarde "1" geschreven De eerste 2 tikken worden meestal al in de fabriek geschreven om de kaart te testen. In het veld van byte 3-4 van de kaart staat dus twee meer dan de uiteindelijke waarde van de kaart als ie verkocht wordt. De waarde op byte 3-4 is BCD gecodeerd. Geldige maten zijn 10, 22, 25, 30, 50, 60, 100 of 150 units. Voor een kaart van 10 units staat dus $8012 op byte 3-4 en voor een kaart van 150 units staat er $6152. Geldige landencodes: $1E Zweden $22 Spanje $30 Noorwegen $33 Andorra $3C Ierland $47 Portugal $55 Tsjechië $5F Gabon $65 Finland
32	248-255	$00

Kaarttype 2

Van de twee verouderde systemen is dit de nieuwste. De kaarten worden op dit moment gebruikt in Nederland, Duitsland en Griekenland en ze worden onder andere gemaakt door de firma's Uniqua, Solaic, Gemplus, Schlumberger en Oldenbourg Kartensysteme. Ze hebben geen 21 Volt programmeerspanning meer nodig en ze zijn iets

slimmer dan de kaarten van type 1. De chips zitten op de ISO-positie.

Kaarttype 2 (ISO positie)



1 Vcc (5V)
2 Reset
3 Clock
4 n.c.
5 Gnd
6 n.c.
7 Data
8 n.c.

n.c.=not connected

Werking

Als je kijkt naar de timing diagrammen op de pagina hiernaast dan valt op dat de interne teller terug gaat naar nul als een clockpuls binnen een resetpuls valt. Zodra de reset weer laag is komt het corresponderende geheugenbit op de output pen te staan. Elke stijgende flank van de clock pen verhoogt de interne teller, maar pas als de clock weer omlaag gaat komt de betreffende bit op de output-pen te staan. (A)
De tellerstand voor de kaart wordt opgeslagen in 5 bytes die als een telraam werken. De stand wordt octaal opgeslagen, de waarde van elke byte in de teller wordt bepaald door het aantal enen in de byte. Kijk maar even naar de memory map (figuur 8). De bits in de teller kunnen naar nul worden geschreven. Een hele byte kan weer op $FF worden geschreven (de waarde neemt dan toe!), maar alleen als er eerst een bit in het register daarboven op nul is gezet. Op zijn best blijft de waarde van de kaart dan dus gelijk. De eerste byte van de teller heeft maar 4 bruikbare bits: de eerste bit (64) is een 'card enable' bitje dat wordt geschreven op het moment dat de kaart geinitialiseerd wordt. De volgende drie bits (65-67) worden soms gebruikt voor tests in het tellergebied tijdens de produktie. De maximale waarde van de teller wordt dus 4096x5, 20480 eenheden. Aangezien een eenheid in Nederland met 1 cent overeenkomt kan er dus theoretisch maximaal fl. 204,80 op een kaart staan.
Als de cel een bit wil schrijven dan loopt hij met clock naar de betreffende bit toe, waarna met een reset puls en een clockpuls de schrijfaktie wordt uitgevoerd. De resetpuls geeft aan dat de schrijfaktie gaat beginnen, en dat de volgende clockpuls niet moet worden gebruikt om de inhoud van het adresregister te verhogen, maar om de schrijfaktie ook daadwerkelijk uit te voeren. (B)
Als de cel een bit wil schrijven en tegelijkertijd de teller-byte 1 stap verder op $FF wil zetten dan wordt doodleuk 2 keer de reset-clock cyclus doorlopen. De eerste keer is een schrijfoperatie, de tweede keer is het de kaart duidelijk dat het onderliggende register op $FF moet worden gezet. (C) Zowel gedurende write als gedurende erase moet de clock minimaal 10 milliseconden worden vastgehouden.
Op de tekening zie je de geheugeninhoud voor dit kaarttype. De issuer code staat in Nederland altijd op $80. De byte met 'specific data' is EEPROM waarin alleen de fabrikant mag schrijven. De documentatie is cryptisch, maar het zou iets met het testen van de chip te

```
void
dotestmode(void)
{
    unsigned char   nw, ow = input_byte();
    unsigned char   ov = DETECT;

    if (verbose)
        printf("Test mode:\n");

    while (1) {
        output(ov);
        printf("\r%s - %s - %s - %s : %s - %s",
         (ov & POWER) ? "Power" : "     ",
         (ov & CLOCK) ? "Clock" : "     ",
         (ov & ISO_RESET) ? "I Reset" : "       ",
         (ov & FRENCH_RESET) ? "F Reset" : "       ",
         (ow & CARD) ? "    " : "Card",
         (ow & I_O) ? "Output" : "      ");
        while ((nw = input_byte()) == ow &&
         !_bios_keybrd(_KEYBRD_READY));
        if (nw == ow) {
            switch (_bios_keybrd(_KEYBRD_READ) &
             0xFF) {
            case 'p':
                ov ^= POWER;
                break;
            case 'r':
                ov ^= ISO_RESET;
                break;
            case 'f':
                ov ^= FRENCH_RESET;
                break;
            case 'c':
                ov ^= CLOCK;
                break;
            case 27:
            case 'q':
                output(0);
                return;
            }
        } else
            ow = nw;
    }
}

void
usage(void)
{
    printf("phone [-cdfhirstv] [-e<n>] [-w<n>]
     [<outputfile>]\n"
           "\t-c\tcontinuous read\n"
           "\t-d\tignore card detect\n"
           "\t-e<n>\twrite bit n and erase
            next byte\n"
           "\t-f\tforce french length\n"
           "\t-h,-?\tthis help\n"
           "\t-i\tinvert input bits\n"
           "\t-r\tread as a real phone\n"
           "\t-s\tsilent mode\n"
           "\t-t\ttest mode\n"
           "\t-v\tverbose mode\n"
           "\t-w<n>\twrite bit n\n");
}

void
main(int argc, char *argv[])
{
    int             write_bit = 0;
    int             erase_bit = 0;
    int             wait_card = 0;
    int             real_read = 0;
    char           *of = NULL;
    int             test = 0;
    char            c;

    pp = *(unsigned int far *) 0x408;  /* LPT1: */
    num_data = 16 * 8;  /* default 128 bit cards */

    while (argc-- > 1) {
        argv++;
        if (argv[0][0] == '-') {
            while ((c = *++(argv[0])) != 0) {
                switch (c) {
                case 'c':
                    go = 1;
                    break;
                case '?':
                case 'h':
                    usage();
                    return;
                case 'f':
                    num_data = 32 * 8;
                    break;
                case 'w':
                    write_bit = atoi(argv[0] + 1);
                    break;
                case 'd':
                    wait_card = 1;
                    break;
                case 'e':
                    erase_bit = atoi(argv[0] + 1);
                    break;
                case 'i':
                    one = !one;
                    break;
                case 'r':
                    real_read = 1;
                    break;
                case 's':
                    silent = 1;
                    break;
                case 't':
                    test = 1;
                    break;
                case 'v':
                    verbose = 1;
                    printf("Phone v1.0\t\t\t\t
              (C)opywrong 1994 by Hack-Tic magazine\n");
                    break;
                }
            }
        } else
            of = argv[0];
    }

    if (verbose)
        printf("Reading on printerport 0x%X\n", pp);

    if (test) {
        dotestmode();
        return;
    }
    initbits();

    output(DETECT);

    while (wait_card &&
!_bios_keybrd(_KEYBRD_READY));
    while (!card_in() &&
!_bios_keybrd(_KEYBRD_READY));

    if (go) {
        while (inp(96) != 1)
            read_data(real_read);
    } else {
        delay(20);

        read_data(real_read);

        if (!silent)
            print_data();
        print_type();

        if (write_bit) {
            delay(20);
            write_bit_iso(write_bit);
            read_data(real_read);
            if (!silent)
                print_data();
            print_type();
        }
        if (erase_bit) {
            delay(20);
            erase(erase_bit);
            read_data(real_read);
            if (!silent)
                print_data();
            print_type();
        }
        if (of) {
            FILE           *f;
            if ((f = fopen(of, "wb")) != NULL) {
                fwrite(data, 1, num_data / 8, f);
                fclose(f);
            } else
                perror(of);
        }
    }
    while (_bios_keybrd(_KEYBRD_READY))
        _bios_keybrd(_KEYBRD_READ);
}
```

la.c

```
#include <stdio.h>
#include <bios.h>
#include <conio.h>
#include <stdlib.h>
#include <dos.h>

unsigned int    pp;

#define POWER       0x40
#define CLOCK       0x20
#define RESET       0x80
#define I_O         0x10

#define ENU_POWER   0xFF

#define output( val )   outp( pp-1, val)
#define input_byte( )   (inp( pp )
 &(POWER|CLOCK|RESET|I_O))
#define keypressed( )   (inp(96)==1)

struct record {
    unsigned long   t;
    unsigned char   val;
};

#define NUMDAT 10000
struct record   the_records[NUMDAT];

void
usage(void)
{
    printf("usage:\tla <filename>\t\t
     for sampling\n"
     "or:\tla -d [-v] <filename>\t
     for dumping\n");
}

void
main(int argc, char *argv[])
{
    unsigned int    count = NUMDAT;
    unsigned long   t = 0;
    struct record   *rp = the_records;
    unsigned char   nc, oc;
    FILE            *f;
    char            *of = NULL;
    struct record   r;
    unsigned long   last = 0;
    int             dump = 0;
    int             verbose = 0;
    int             c;

    while (argc-- > 1) {
        argv++;
        if (argv[0][0] == '-')
            switch (argv[0][1]) {
            case '?':
            case 'h':
                usage();
                return;
            case 'd':
                dump = 1;
                break;
            case 'v':
                verbose = 1;
                break;
            }
        else
            of = argv[0];
    }

    if (of == NULL) {
        usage();
        return;
    }
    f = fopen(of, "rb");
    if (dump) {
        printf("Dump of file '%s':\n",
         of);
        if (f != NULL) {
            count = 0;
            oc = POWER | CLOCK | I_O;
            while (fread(&r,
  sizeof(struct record), 1, f) == 1) {
                if (verbose) {
printf("%9lu:  %s  .  %s  .  %s  .
 %s\n", r.t - last,
 (r.val & POWER) ? ((oc & POWER) ? " " :
 "-") : ((oc & POWER) ? "+" : " "),
 (r.val & RESET) ? ((oc & RESET) ? " " :
 "+") : ((oc & RESET) ? "-" : " "),
 (r.val & CLOCK) ? ((oc & CLOCK) ? " " :
 "-") : ((oc & CLOCK) ? "+" : " "),
 (r.val & I_O) ? ((oc & I_O) ? " " :
 "-") : ((oc & I_O) ? "+" : " "));
printf("          %s . %s . %s . %s\n",
 (r.val & POWER) ? "     " : "Power",
 (r.val & RESET) ? "Reset" : "     ",
 (r.val & CLOCK) ? "     " : "Clock",
 (r.val & I_O) ? "   " : "I/O");
                    oc = r.val;
                } else {
                    printf("%9lu:\t%s -
                     %s - %s - %s\n",
                     r.t - last,
                     (r.val & POWER) ?
                     "     " : "Power",
                     (r.val & RESET) ?
                     "Reset" : "     ",
                      (r.val & CLOCK) ?
                     "     " : "Clock",
                      (r.val & I_O) ?
                     "   " : "I/O");
                }
```

```
            last = r.t;
            count++;
        }
        fclose(f);
        printf("File contained %u
         samples.\n", count);
    } else
        perror(argv[1]);
} else {
    if (f != NULL) {
        fclose(f);
        printf("File '%s' exists,
         overwrite (y/n)? \7", of);
        while (1) {
    c = _bios_keybrd(_KEYBRD_READ) &
             0xff;
            if (c == 'y') {
                printf("y\n");
                break;
            }
            if (c == 'n') {
          printf("n\nCancelled.\n");
                return;
            }
            printf("\7");
        }
    }
    pp = (*(unsigned int far *)
0x408) + 1; /* look for LPT1: */
    printf("Starting sampling on port
     0x%X...\n", pp - 1);
    output(EMU_POWER);
    oc = input_byte();
    _disable();
    while (count) {
        do
            t++;
        while ((nc = input_byte()) ==
         oc && !keypressed());
        if (keypressed())
            break;
        rp->val = oc = nc;
        rp->t = t;
        rp++, count--;
    }
    _enable();
    if ((f = fopen(of, "wb")) !=
     NULL) {
        fwrite(the_records,
         sizeof(struct record),
         NUMDAT - count, f);
        fclose(f);
    } else
        perror(argv[1]);
    printf("%u samples stored in
     '%s'.\n", NUMDAT - count, of);
    output(0);
  }
}
```

Deze programma's staan op XS4ALL !

Hack-Tic tijdschrift heeft een eigen subdirectory op XS4ALL. In /pub/magazine staan alle listings die we vanaf nu afdrukken. phone.c en la.c staan er, en ook de gecompileerde versies staat erbij. We proberen zo snel mogelijk ook de sources uit vroegere Hack-Tic's in /pub/magazine neer te zetten.
Via XS4ALL kun je ook gebruik maken van het hele Internet. Om een account aan te vragen bel je met je modem naar telefoonnummer 020-6222175 (max. V32bis - 14.400 bps) of naar 020-6265060 (max. ZyXEL 19.200 bps) en meld je je aan als 'new'. Daarna gewoon de instructies op het scherm volgen en de acceptgiro (75 gulden / 3 maanden) betalen. Je kunt natuurlijk ook wachten tot de files op je favoriete bbs verschijnen (kan nooit lang duren).

http://www.hacktic.nl/magazine

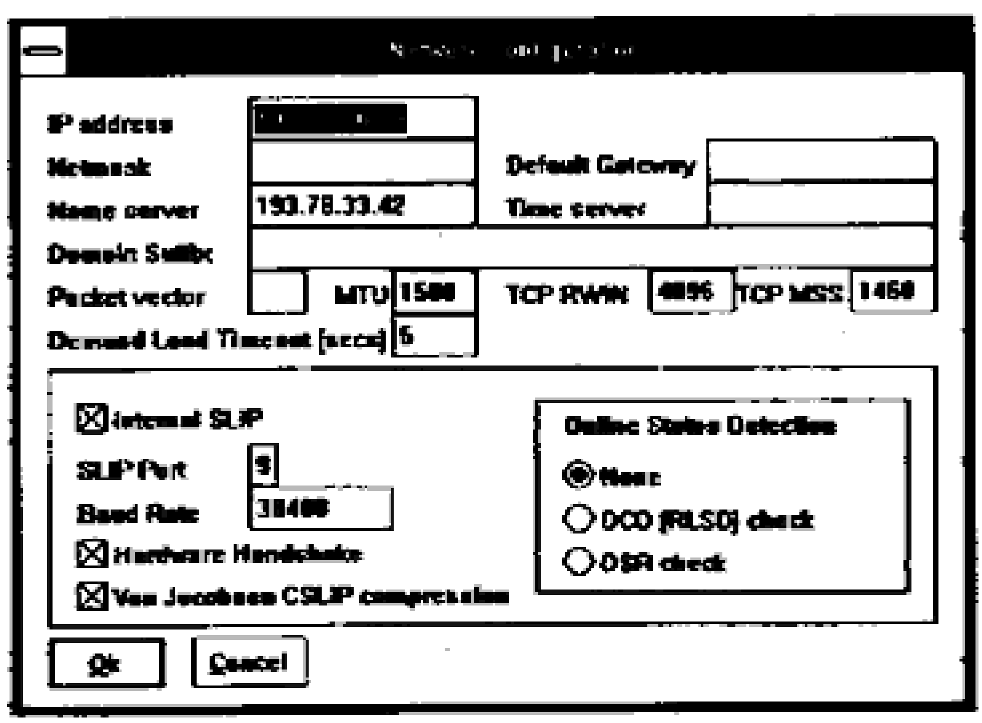
Ergens in september '94 heeft Hack-Tic Tijdschrift zijn eigen World Wide Web pagina's op het bovenstaande adres. Het ziet er het mooiste uit als je over een Internet verbinding en het programma Mosaic beschikt. Zie het artikel over Winsock en Mosaic elders in deze Hack-Tic.

Internet thuis

De Internet-gemeenschap is te lang gespleten geweest: of je had een duur state-of-the-art workstation van 15 mille en dan was Internet een genot voor de muisklikkende gebruiker. Voor die gebruikers zat het net vol met plaatjes, filmpjes en geluidjes. Aan de andere kant had je mensen die met een modem en een PC inbelden en met vt-100 terminalemulatie genoegen moesten nemen. Deze mensen waren al heel blij als ze de vier cursortoetsen konden gebruiken. Geen plaatjes, geen geluidjes, alleen tekst, 80 bij 24 tekens welteverstaan.
Sinds enige tijd zijn er ook voor gewone PC's 'client'-programma's die de zaken mooier in beeld (en geluid) brengen. Een aantal van die programma's willen we in dit artikel bespreken en laten zien. Alle in dit artikel beschreven programma's draaien onder Microsoft Windows. MS-Windows is een SOS, een zogenaamd Schijt Operating System, maar op de PC helaas de standaard voor een grafische omgeving. Als je niet aan de gang wilt met Unix en X-windows (beter, maar vereist een hoop kennis) is dit je enige keus.
Alle onderstaande programma's zijn public-domain of shareware en her en der op het Internet te vinden. Ze staan onder andere in de directory /pub op Xs4all.

Internet verbinding

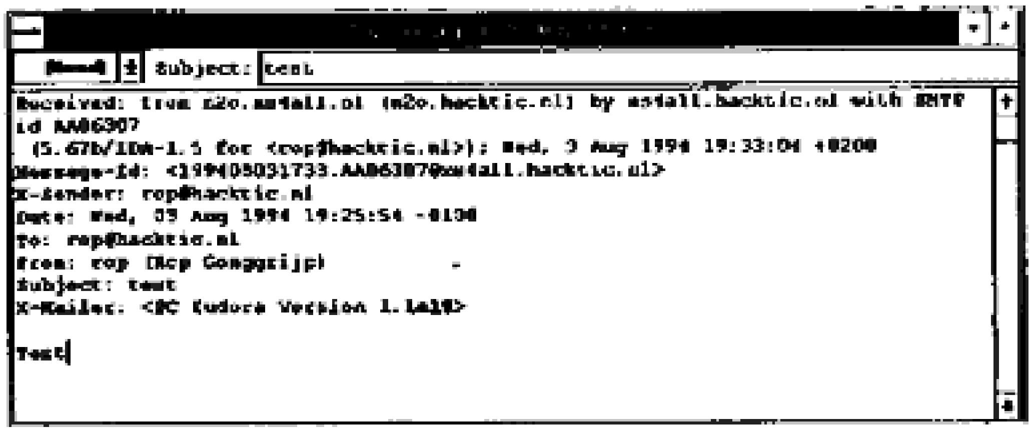
Allereerst zullen de programma's die onder MS-Windows draaien verbinding moeten kunnen maken met het Internet. Daarvoor gebruik je het Winsock (Windows Sockets) mechanisme. De file 'winsock.dll' is de schakel tussen de programma's die 'op het net' willen en de feitelijke netwerk-link.
Als je zelf beschikt over een ethernet dat al aan het Internet hangt is de hele zaak vrij makkelijk: zoek een bij jouw netwerkdrivers passende winsock.dll. De kans is echter vrij groot dat je thuis geen ethernetaansluiting op het Internet hebt. In dat geval kun je gebruik maken van een protocol dat SLIP heet. Met SLIP (Serial Line Internet Protocol). Op het Internet verpakt iedereen zijn data in zgn. IP-pakketjes. Door die weer verder in te pakken kun je deze pakketjes over een seriële lijn (en dus over een modemverbinding) verzenden.
Veel Internet-aanbieders bieden SLIP aan in hun pakket, en als je (liefst binnen je basistariefgebied) een aanbieder hebt gevonden waar je kunt SLIPpen, dan kun je aan de slag.



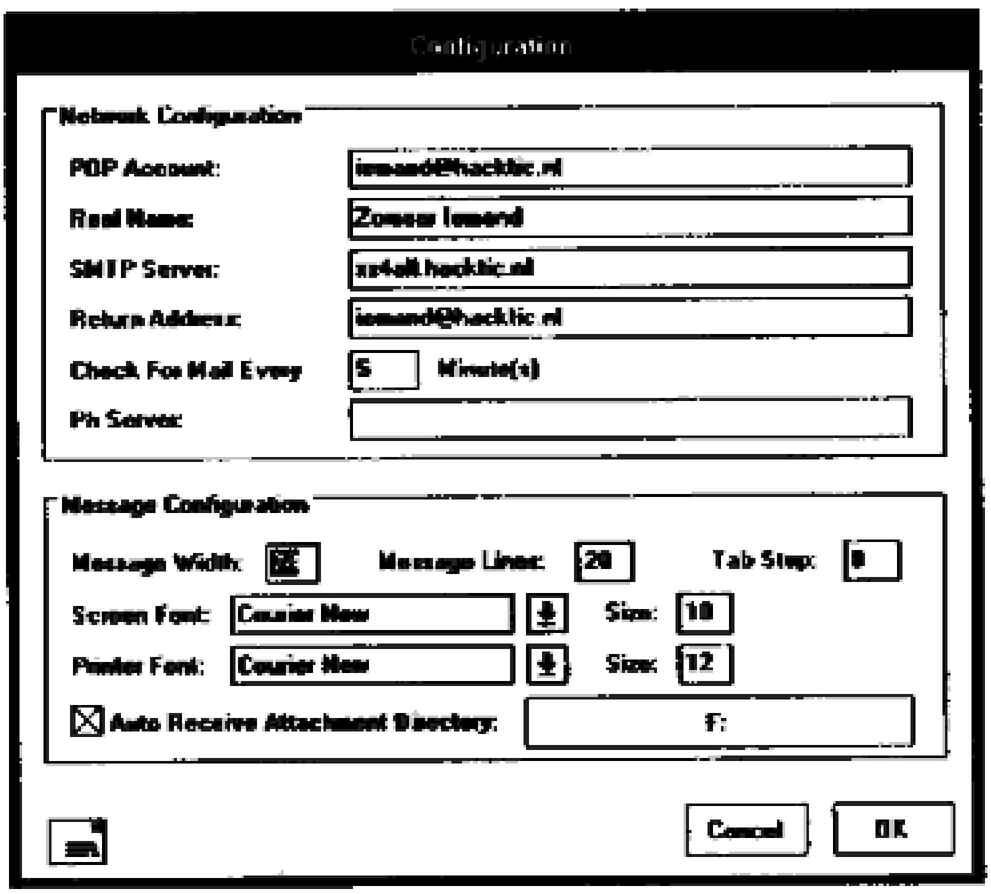
Trumpet Winsock Driver

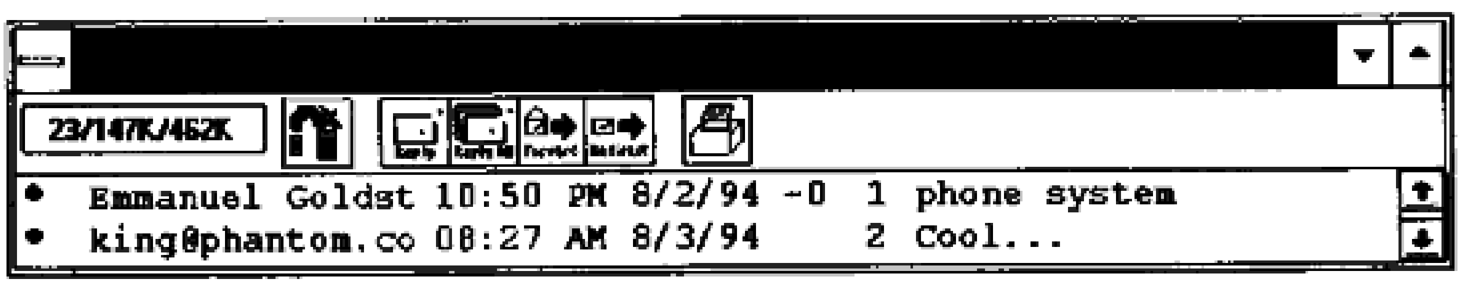
Allereerst heb je een programma nodig dat de feitelijke verbinding maakt. Trumpet Winsock is zo'n programma. Bijna alles is instelbaar, en je kunt zowel met de hand als vanuit een script kiezen en inloggen. Op de pagina hiernaast zie je het configuratiewindow van de Trumpet driver. Als dit programma eenmaal de verbinding heeft opgebouwd dan kunnen alle andere programma's het net gebruiken.

Eudora mail



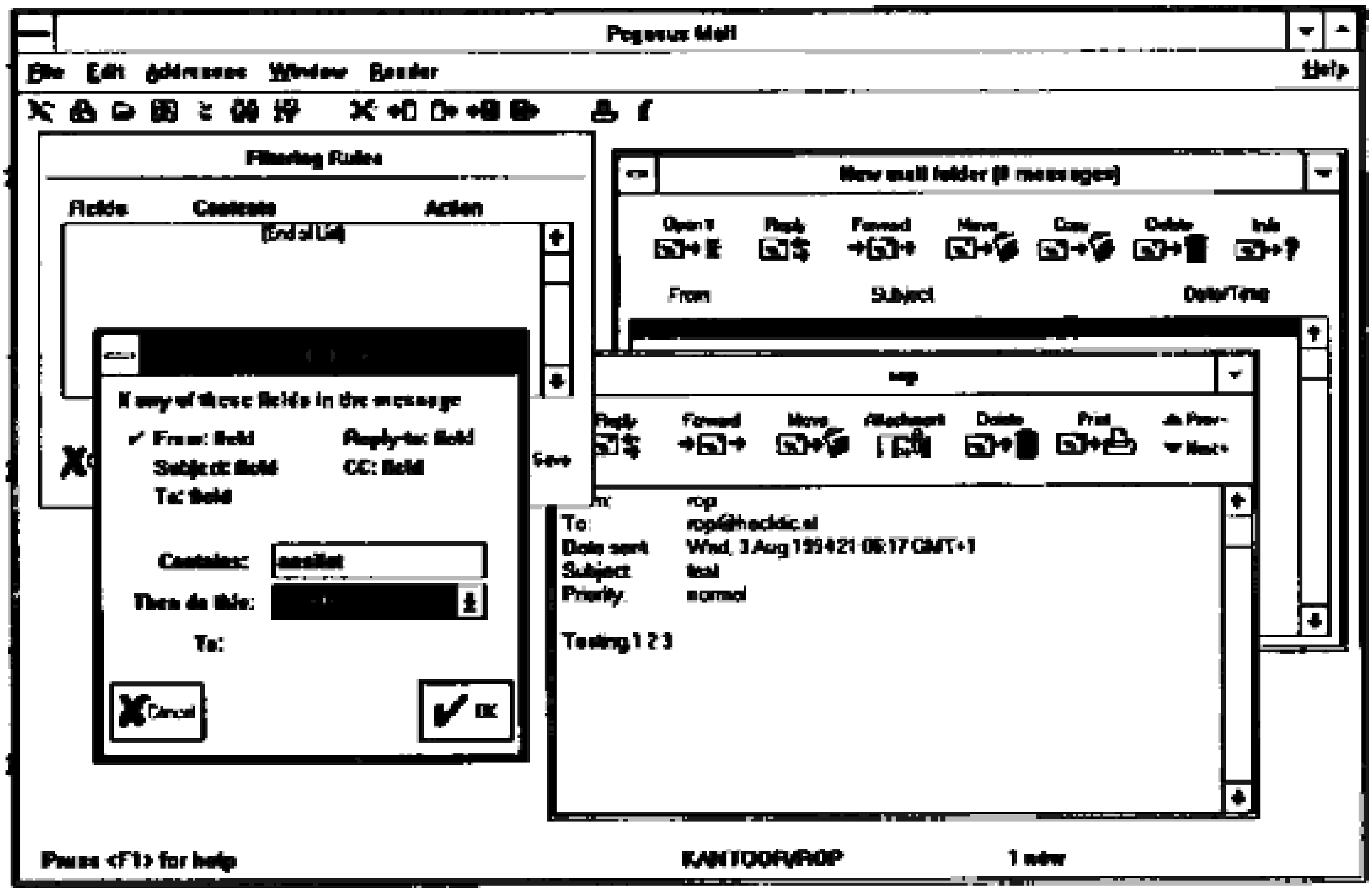
Eudora is een mailreader die gebruik maakt van het POP-protocol om je mail op te halen. De meeste Internet aanbieders ondersteunen POP. Je kunt met Eudora electronische post lezen en schrijven. De post kan in folders worden opgeborgen en je kunt lijstjes aanmaken van mensen die je vaker mail stuurt. Op zich een aardig programma, maar er zijn beperkingen. Zo is de editor voor het invoeren van berichten bepaald spartaans, en is het wat al te gemakkelijk om je hele ingetikte bericht kwijt te raken. Ook het verder sturen van berichten (forwarding) werkt een beetje typisch.



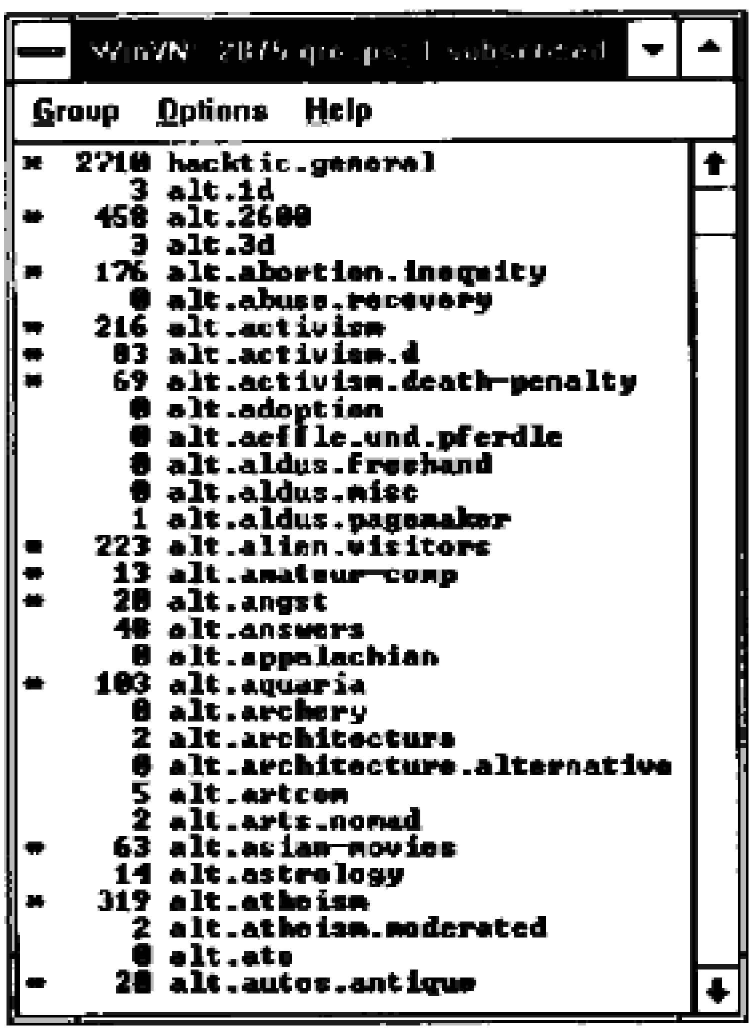


Pegasus Mail voor Windows

P-mail voor Windows is ook een POP-mailreader, maar dan met veel meer mogelijkheden. Je kunt headers scannen, en dan op grond van bijvoorbeeld de afzender beslissen om de mail in een bepaalde folder op te slaan of zelfs weg te gooien. Ideaal voor mensen die vinden dat ze te veel mail krijgen.



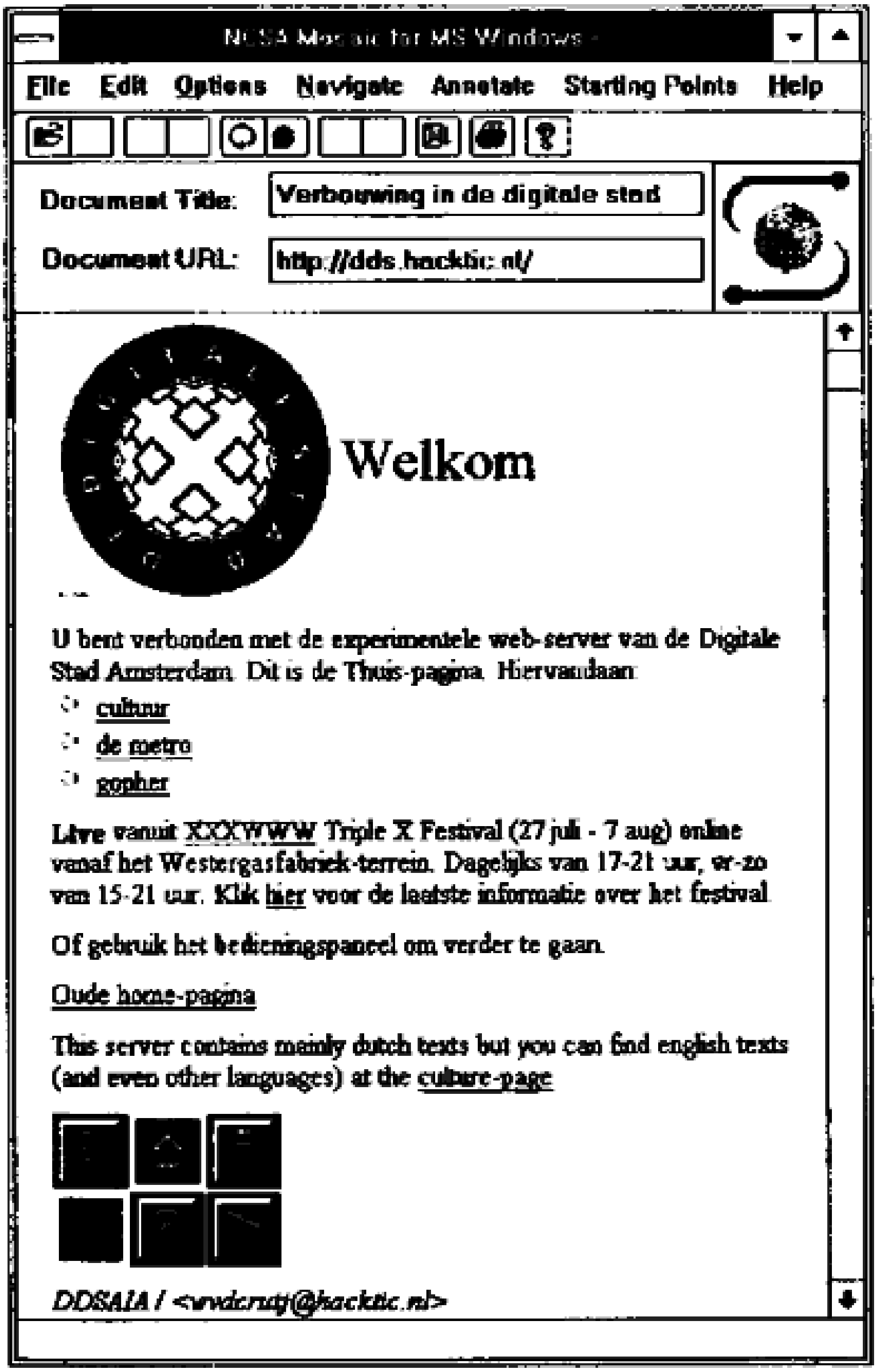
WinVN newsreader



WinVN is een newsreader voor UseNet newsberichten die werkt met het NNTP protocol om berichten van het net te halen. Aardig, maar beslist niet mooi genoeg. WinVN haalt bijvoorbeeld elke keer dat je een newsgroup binnengaat alle headers van berichten op (duurt te lang over een modemverbinding). Verder missen essentiële features. In deze dagen van netvervuiling heeft iedereen een kill-file nodig om aan te geven wiens berichten je niet meer wilt zien. Ook de editor om dingen te posten lijkt nergens op. Het werkt, en er is mee te leven, maar er zou iemand een echt mooie newsreader voor Winsock moeten maken.

Mosaic (World Wide Web)

Mosaic is een programma waarmee je WWW (World Wide Web) pagina's kunt bekijken.Om een voorbeeld te geven van zo'n World Wide Web-pagina is de home-page van De Digitale Stad hieronder afgebeeld. Elke pagina kan plaatjes en tekst, maar ook beeld en animatie met elkaar combineren, en elk element kan weer naar andere pagina's verwijzen, zodat je al klikkend op je muisknop over het net zoeft. Op het Internet is op die manier een soort wereldwijde hypertext onstaan: iedereen verwijst naar elkaars pagina's dat het een lieve lust is. Als je gaat spelen met Mosaic is 1 ding wel heel snel duidelijk: een snel modem is een must. Moet je eens opletten hoe langzaam je de nieuwste, mooiste, snelste modems vindt.



Tijdens de inslagen van de komeet Shoemacher-Levy 9 op Jupiter waren er op allerlei plaatsen in de wereld via WWW mooie plaatjes te bekijken. De belangstelling was zo groot dat de astronomische instituten die de informatie op het net zetten de vraag bij lange na niet aankonden. Zoals gezegd: WWW vreet nogal wat bandbreedte.
Terug naar Mosaic:zeker de mooiste WWW-viewer die er is. Je kunt er echter niet alleen WWW-pagina's mee bekijken, je kunt er ook gegevens mee bekijken en ophalen die in FTP- (File Transfer Protocol) of Gopher (wereldwijd menusysteem) formaat zijn opgeslagen, en je kunt er UseNet news mee lezen. Heel, heel, heel mooi.

Rop

Underground On-Line

Op de volgende plekken op het net zijn (soms) leuke computer-underground dingen te beleven. Aanvullingen op de onderstaande lijst (ook leuke ftp-sites en WWW-pagina's) naar de redaktie.

IRC chatkanalen

#2600	van de mensen van 2600 Magazine,meeting 26ste van elke maand
#hack, #warez	Vaak invitation only, soms puberale egotripperij
#phreak	Aardig, maar eigenlijk alleen over Amerikaanse telefoonnet

UseNet newsgroups

hacktic.*, alt.2600, comp.dcom.telecom, comp.risks, comp.security.*, sci.electronics, alt.cyberpunk, alt.privacy, alt.privacy.clipper, comp.org.eff.talk

Utopia Weg

In januari 1992 ontstond het Hacktic netwerk door de eerste UUCP-verbindingen tussen de UvA, Hacktic-HQ en Utopia BBS. De belangstelling en het enthousiasme waren meteen enorm en het netwerk nam een grote vlucht. Nu, 2 jaar later, zijn er bijna 250 UUCP-nodes, een Xs4all public Unix met 24 lijnen, een Digitale Stad met 40 lijnen, razendsnelle Internet verbindingen en het zelfde enthousiasme. Dit alles betekent ook meer mensen, meer projecten, meer e-mail en meer vergaderingen.
Utopia heeft in de tijd van haar bestaan verschillende functies gehad. Allereerst was het een systeem voor de computer-underground in Nederland. Een plaats waar je met andere phreaks kon e-mailen, chatten en informatie uitwisselen. Daarna is het steeds meer een systeem geworden waar je kon e-mailen en UseNet news kon lezen. Die functie is nu overbodig geworden i.v.m. de komst van Xs4all en De Digitale Stad. Daarnaast heeft Utopia in het Hacktic netwerk een belangrijke functie gehad als UUCP-gateway. In de drukke tijden had Utopia meer dan 75 uucp-nodes onder zich hangen.
Het laatste jaar is de hoeveelheid tijd en werk die in het Hacktic netwerk is gaan zitten enorm toegenomen. Vanaf december, toen de voorbereidingen van De Digitale Stad een grote vlucht namen, is de service van Utopia daardoor in het geding gekomen. Ik heb sterk het gevoel dat dit in de laatste maanden van het bestaan van utopia alleen erger is geworden. Hiervan werden de UUCP-nodes die bij Utopia pollen de dupe, evenals de gebruikers die nog naar utopia bellen. Er was nauwelijks tijd om newsgroups aan te sluiten, en soms moesten mensen onaanvaardbaar lang wachten totdat dit was gebeurd.
Door deze omstandigheden was ik genoodzaakt om mijn activiteiten voor Utopia bbs helemaal te staken. Er lag ander werk te wachten dat voor mij meer prioriteit had. De Digitale Stad en Xs4all vragen steeds meer tijd en daarnaast zijn er altijd nieuwe experimenten en projecten die aandacht verdienen. De UUCP nodes krijgen bij Xs4all de facto een betere service. Utopia bestaat niet meer.

Felipe Rodriquez <felipe@hacktic.nl>

Auto Weg

In de kranten stond onlangs het verhaal van een autodief die was aangehouden omdat hij met behulp van een 'speciaal apparaat' in staat was om auto's te jatten die voorzien waren van een alarm/deuropener met infrarode afstandsbediening. Soms stal hij alleen de radio's en deed daarna de deuren weer netjes dicht en het alarm aan. Juist dat laatste maakt de politie nieuwsgierig.
Wat blijkt: het 'speciale apparaat' is een doodgewone 'learning remote-control' die je bij elke electro-zaak voor onder de 100 piek op de kop kunt tikken. Even wachten tot de eigenaar de zaak afsluit, knopje drukken en voila.

Nieuwe PTT diensten

20 jaar nadat de meeste Amerikanen call-forwarding al weer ouderwets vonden kwam de PTT met haar moderne dienst *21. Hieronder een aantal (topgeheime) features die in het PTT-dienstenpakket voor 1995 zitten.

*30 Hold Disrupt

Als je meer dan 15 seconden in de wacht gezet wordt dan klinkt er aan de andere kant een luide gedigitaliseerde stem uit de speaker. "Hee, ik heb niet de hele dag de tijd!". 'Music-on-hold' installaties worden door deze dienst uitgeschakeld.

*31 Fopspeen

Zit je vast aan een kennis die alleen maar even wil dat je luistert? Met de fopspeen dienst kun je met een druk op de knop zorgen dat elke pauze opgevuld wordt met een vantevoren opgenomen 'Aha', 'Juist' of 'Jaja'.

*32 Fopspeen +

Pleegt automatisch al je beleefdheidstelefoontjes en kijkt of er nog nieuwtjes zijn.

*33 Tele-ontslag

Kunt u de stress van de volgende ontslag-golf niet meer aan? Met *33, gevolgd door het toestelnummer van een werknemer kunt u de betreffende persoon ontslaan. De boekhouding, de personeelsafdeling en de werknemer in kwestie worden automatisch op de hoogte gesteld.

*34 Internal Security Notification

Een absolute must voor de manager die wil weten wat er binnen zijn bedrijf gebeurt. Als iemand binnen uw bedrijf uw naam noemt in een conversatie dan krijgt U het betreffende gesprek automatisch in uw voice-mail box om het na te luisteren.

*35 Selectief Ontmoedigen

Programmeer de nummers van mensen die u ECHT niet wilt spreken. Als ze uw nummer kiezen krijgen ze via de hoorn van hun toestel een electrische schok.

*36 Schat, je denkt ook aan alles!

Sla verjaardagen en andere belangrijke data op met *36. Op die dag belt de dienst uw warme relaties om ze (met uw stem) van uw diepste genegenheid te overtuigen.

*37 Subliminafoon

Gedurende een gesprek worden voortdurend zinnen als 'Zeg ja' of 'Verhoog mijn salaris' afgespeeld, maar net te zacht om ze bewust te horen.

Vrij naar David.Gersic@t70.n11.z1.fidonet.org

Gratis bellen in cellen deel V

Veel telefooncellen denken nog steeds dat je alles gratis mag bellen dat met 008 begint, omdat dat 'vroeger' het informatienummer was. Nu 00 het nieuwe internationale toegangsnummer is kun je dus vanuit sommige cellen (vooral muntcellen met een LCD-schermpje die guldens en kwartjes accepteren) gratis bellen met alle landen waarvan het landnummer met een 8 begint. Ook Inmarsat is te bellen (tot ca. fl. 15,05 per minuut!). Gebruik maken van dit lek is wellicht niet eens illegaal: je kunt immers bij zo'n cel niet voor dit gesprek betalen, tenzij je (wellicht wel strafbare) truukjes uit zou halen. Maar bedenk: wij zijn allemaal technici, geen juristen.

Het ligt voor de hand dat deze eigenschap niet in het evolutionaire voordeel van zo'n cel werkt en dat de overgebleven cellen van dit type in het wild vrij snel door beter aangepaste versies zullen worden verdrongen. Dit proces is het verst gevorderd in stedelijke gebieden, waar de verschillende soorten het hardst concurreren.

Zomaar een lijstje met wat landencodes

81	Japan
84	Vietnam
850	Noord-Korea
852	Hongkong
855	Cambodja
856	Laos
86	China
871	Inmarsat East Atlantic
872	Inmarsat Pacific
873	Inmarsat Indian
874	Inmarsat West Atlantic
880	Bangladesh
886	Taiwan

Hack-Tic wil veel meer weten over:

GSM
Greenpoint
de 06-centrale

postbus 22953
1100 DL Amsterdam

In deze paper-superhighway:

Chipcard Hacking

Weer kleinere batch-virussen.

Wet cryptografie even van de baan

Wat is er te doen op het Internet?

Strafzaak tegen hackers mislukt

Je eigen pc op het net zetten

Heel veel lezerspost

en meer !

